



FortiOS - Cookbook

Version 6.2.15

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



June 08, 2023

FortiOS 6.2.15 Cookbook

01-6215-538742-20230608

TABLE OF CONTENTS

Change Log	16
Getting started	17
Differences between models	17
Using the GUI	17
Connecting using a web browser	17
Menus	18
Tables	19
Entering values	21
Using the CLI	22
Connecting to the CLI	23
CLI basics	25
Command syntax	31
Subcommands	34
Permissions	36
FortiExplorer for iOS	36
Getting started with FortiExplorer	37
Connecting FortiExplorer to a FortiGate via WiFi	40
Running a security rating	41
Upgrading to FortiExplorer Pro	42
Basic administration	42
Registration	43
FortiCare and FortiGate Cloud login	46
FortiGate Cloud	49
Troubleshooting your installation	51
Zero touch provisioning	53
Zero touch provisioning with FortiDeploy	53
Zero touch provisioning with FortiManager	56
Dashboard	58
Dashboard CLI	61
Configuration backups	62
Fortinet Security Fabric	67
Security Fabric settings and usage	67
Components	68
Configuring the root FortiGate and downstream FortiGates	70
Configuring FortiAnalyzer	75
Configuring other Security Fabric devices	76
Using the Security Fabric	90
Deploying the Security Fabric	103
Security Fabric over IPsec VPN	111
Leveraging LLDP to simplify Security Fabric negotiation	117
Configuring the Security Fabric with SAML	120
Configuring single-sign-on in the Security Fabric	120
CLI commands for SAML SSO	125
SAML SSO with pre-authorized FortiGates	126

Navigating between Security Fabric members with SSO	126
Advanced option - FortiGate SP changes	129
Advanced option - unique SAML attribute types	129
Security rating	133
Security Fabric score	135
Comprehensive report extensions	135
Verifying FortiAnalyzer configurations	138
Fabric connectors	139
SDN connectors	140
Kubernetes (K8s) SDN connectors	182
SSO/Identity connectors	197
Threat feeds	218
Automation stitches	233
Creating automation stitches	234
Triggers	237
Actions	242
Execute a CLI script based on CPU and memory thresholds	264
Troubleshooting	269
Viewing a summary of all connected FortiGates in a Security Fabric	269
Diagnosing automation stitches	272
FortiView	276
FortiView interface	276
Time display	277
FortiView filters	277
Drill down to details	277
View selection	278
FortiView from disk	279
FortiView from FortiAnalyzer	282
Cloud application view	284
Viewing cloud applications	284
Configuring the Cloud Applications widget	289
Cloud application view examples	293
FortiView Sources usability	298
FortiView from FortiGate Cloud	299
Supported views for different log sources	302
FortiGate Cloud-based IOC	303
FortiView — subnet filters	304
FortiView dashboards and widgets	305
FortiView object names	310
Network	315
Interfaces	315
Interface settings	316
Aggregation and redundancy	319
VLANs	321
Enhanced MAC VLANs	327
Inter-VDOM routing	330
Software switch	335

Hardware switch	337
Zone	338
Virtual Wire Pair	340
Virtual switch support for FortiGate 300E series	342
Failure detection for aggregate and redundant interfaces	344
VLAN inside VXLAN	344
Virtual Wire Pair with VXLAN	347
Interface MTU packet size	348
One-arm sniffer	351
DNS	352
Important DNS CLI commands	352
DNS domain list	353
FortiGate DNS server	355
DDNS	357
DNS latency information	360
DNS over TLS	362
DNS troubleshooting	362
Explicit and transparent proxies	363
Explicit web proxy	364
FTP proxy	366
Transparent proxy	368
Proxy policy addresses	371
Proxy policy security profiles	379
Explicit proxy authentication	385
Transparent web proxy forwarding	391
Multiple dynamic header count	392
Restricted SaaS access (Office 365, G Suite, Dropbox)	395
Explicit proxy and FortiSandbox Cloud	397
DHCP server	400
IP address assignment with relay agent information option	402
Static routing	405
Routing concepts	405
Policy routes	415
Equal cost multi-path	417
Dual internet connections	421
Multicast	427
Multicast routing and PIM support	427
Configuring multicast forwarding	428
Direct IP support for LTE/4G	431
LLDP reception	434
NetFlow	436
Verification and troubleshooting	438
NetFlow templates	438
SD-WAN	451
SD-WAN quick start	451
Configuring the SD-WAN interface	452
Adding a static route	454
Selecting the implicit SD-WAN algorithm	454

Configuring security policies for SD-WAN	455
Link monitoring and failover	455
Results	457
Configuring SD-WAN in the CLI	461
WAN path control	463
Performance SLA - link monitoring	463
Performance SLA - SLA targets	465
Factory default health checks	466
Implicit rule	469
SD-WAN rules - best quality	472
SD-WAN rules - lowest cost (SLA)	475
SD-WAN rules - maximize bandwidth (SLA)	477
Application steering using SD-WAN rules	480
SD-WAN traffic shaping and QoS	492
Per-link controls for policies and SLA checks	496
DSCP tag-based traffic steering in SD-WAN	498
Advanced configuration	509
Self-originating traffic	509
SDN dynamic connector addresses in SD-WAN rules	512
Forward error correction on VPN overlay networks	515
Using BGP tags with SD-WAN rules	518
BGP multiple path support	521
Controlling traffic with BGP route mapping and service rules	523
Applying BGP route-map to multiple BGP neighbors	530
ADVPN and shortcut paths	536
DSCP matching (shaping)	549
Dual VPN tunnel wizard	552
SD-WAN with FGCP HA	555
Enable dynamic connector addresses in SD-WAN policies	561
SD-WAN cloud on-ramp	562
Configuring the VPN overlay between the HQ FortiGate and cloud FortiGate-VM	562
Configuring the VPN overlay between the HQ FortiGate and AWS native VPN gateway	567
Configuring the VIP to access the remote servers	571
Configuring the SD-WAN to steer traffic between the overlays	573
Verifying the traffic	577
Hub and spoke SD-WAN deployment example	584
Datacenter configuration	585
Branch configuration	590
Validation	595
Dynamic definition of SD-WAN routes	596
Adding another datacenter	597
Configuring SD-WAN in an HA cluster using internal hardware switches	598
HA failover	598
Failure on a hardware switch or ISP router	599
Configuration	599
Troubleshooting SD-WAN	601
Tracking SD-WAN sessions	602

Understanding SD-WAN related logs	602
SD-WAN related diagnose commands	605
SLA logging	609
SLA monitoring using the REST API	611
SD-WAN bandwidth monitoring service	613
System	617
Basic system settings	617
Advanced system settings	617
Operating modes	618
Administrators	619
Administrator profiles	619
Add a local administrator	621
Remote authentication for administrators	621
Password policy	624
Associating a FortiToken to an administrator account	625
Firmware	626
Downloading a firmware image	626
Testing a firmware version	627
Upgrading the firmware	628
Downgrading to a previous firmware version	629
Installing firmware from system reboot	630
Restoring from a USB drive	631
Controlled upgrade	632
Settings	632
Default administrator password	633
Changing the host name	633
Setting the system time	634
Configuring ports	637
Setting the idle timeout time	638
Setting the password policy	638
Changing the view settings	638
Setting the administrator password retries and lockout time	639
TLS configuration	640
Controlling return path with auxiliary session	641
Email alerts	644
Trusted platform module support	648
Virtual Domains	650
Split-task VDOM mode	651
Multi VDOM mode	655
Configure VDOM-A	658
Configure VDOM-B	660
Configure the VDOM link	663
Configure VDOM-A	667
Configure VDOM-B	669
High Availability	671
Introduction to the FGCP cluster	672
Failover protection	673
HA heartbeat interface	674

FGSP (session synchronization) peer setup	683
Synchronizing sessions between FGCP clusters	684
Firmware upgrades in FGSP	685
Using standalone configuration synchronization	686
Troubleshoot an HA formation	687
Check HA sync status	688
Disabling stateful SCTP inspection	690
Upgrading FortiGates in an HA cluster	691
Out-of-band management with reserved management interfaces	692
In-band management	697
HA cluster setup examples	698
SNMP	707
Interface access	707
MIB files	708
SNMP agent	708
SNMP v1/v2c communities	709
SNMP v3 users	710
Important SNMP traps	712
Replacement messages	713
Replacement message images	714
Modifying replacement messages	715
Replacement message groups	717
Example	718
FortiGuard	720
IPv6 FortiGuard connections	721
Configuring antivirus and IPS options	722
Manual updates	722
Automatic updates	723
Sending malware statistics to FortiGuard	725
Update server location	725
Filtering	726
Override FortiGuard servers	727
Online security tools	727
FortiGuard third party SSL validation and anycast support	728
Configuration scripts	730
Workspace mode	730
Feature visibility	732
Security feature presets	732
Certificates	733
Uploading a certificate using the GUI	733
Uploading a certificate using the CLI	736
Uploading a certificate using an API	737
Procure and import a signed SSL certificate	741
Microsoft CA deep packet inspection	745
Provision a trusted certificate with Let's Encrypt	750
Creating certificates with XCA	753
RAID	761
Conserve mode	764

Proxy inspection in conserve mode	764
Flow inspection in conserve mode	765
Diagnostics	765
Policy and Objects	767
Policies	767
Firewall policy parameters	768
Profile-based NGFW vs policy-based NGFW	768
NGFW policy mode application default service	773
Policy views and policy lookup	775
Policy with source NAT	776
Policy with destination NAT	786
Policy with Internet Service	799
NAT64 policy and DNS64 (DNS proxy)	814
NAT46 policy	818
Local-in policies	821
DoS protection	822
IPv4/IPv6 access control lists	830
Mirroring SSL traffic in policies	831
Inspection mode per policy	831
Combined IPv4 and IPv6 policy	834
FortiGuard DNS filter for IPv6 policies	835
OSPFv3 neighbor authentication	837
Firewall anti-replay option per policy	839
Enabling advanced policy options in the GUI	839
Recognize anycast addresses in geo-IP blocking	840
Authentication policy extensions	841
NTLM extensions	842
HTTP to HTTPS redirect for load balancing	845
Use active directory objects directly in policies	847
FortiGate Cloud / FDN communication through an explicit proxy	850
Objects	852
Address group exclusions	852
MAC addressed-based policies	854
Dynamic policy — fabric devices	856
FSSO dynamic address subtype	858
ClearPass integration for dynamic address objects	862
Using wildcard FQDN addresses in firewall policies	866
VIP groups	869
Traffic shaping	870
Determining your QoS requirements	871
Packet rates	873
Interface bandwidth limit	874
Changing traffic shaper bandwidth unit of measurement	875
Shared traffic shaper	876
Per-IP traffic shaper	880
Type of Service-based prioritization and policy-based traffic shaping	883
Interface-based traffic shaping profile	886
Classifying traffic by source interface	894
Configuring traffic class IDs	895

Traffic shaping schedules	897
QoS assignment and rate limiting for quarantined VLANs	899
Weighted random early detection queuing	900
Security Profiles	907
Antivirus	907
Content disarm and reconstruction for antivirus	908
FortiGuard outbreak prevention for antivirus	911
External malware block list for antivirus	913
Checking flow antivirus statistics	916
CIFS support	918
Databases	925
Using FortiSandbox appliance with antivirus	926
Using FortiSandbox Cloud with antivirus	936
Web filter	947
URL filter	948
FortiGuard filter	954
Usage quota	961
Web content filter	963
File filter	967
Advanced filters 1	973
Advanced filters 2	977
External resources for web filter	982
Reliable web filter statistics	988
Flow-based web filtering	991
URL certificate blocklist	993
DNS filter	998
DNS filter behavior in proxy mode	998
How to configure and apply a DNS filter profile	999
FortiGuard category-based DNS domain filtering	1002
Botnet C&C domain blocking	1006
DNS safe search	1009
Local domain filter	1011
DNS translation	1014
Using a FortiGate as a DNS server	1017
Troubleshooting for DNS filter	1018
Application control	1021
Basic category filters and overrides	1022
Port enforcement check	1026
Protocol enforcement	1027
Intrusion prevention	1028
Signature-based defense	1030
IPS configuration options	1033
Botnet C&C IP blocking	1037
Email filter	1041
HELO DNS lookup	1042
Return email DNS check	1042
Block/allow list	1042
Banned words	1043

Trusted IP addresses	1044
MIME header	1045
Configuring a local-based email filter	1046
FortiGuard-based filters	1048
Third-party-based filters	1050
File type-based filters	1050
Filtering order	1056
Protocols and actions	1057
Configuring webmail filtering	1058
Data leak prevention	1059
Basic DLP filter types	1060
DLP fingerprinting	1062
VoIP solutions	1066
General use cases	1067
SIP message inspection and filtering	1070
SIP pinholes	1072
SIP over TLS	1073
Custom SIP RTP port range support	1074
Voice VLAN auto-assignment	1075
ICAP	1077
ICAP configuration example	1078
Web application firewall	1080
Protecting a server running web applications	1081
Inspection modes	1084
About inspection modes	1084
SSL Inspection	1091
SSH traffic file scanning	1098
Overrides	1101
Web rating override	1102
Web profile override	1107
Custom signatures	1111
Application groups in policies	1111
VPN	1114
IPsec VPNs	1114
General IPsec VPN configuration	1114
Site-to-site VPN	1139
Remote access	1199
Aggregate and redundant VPN	1245
Overlay Controller VPN (OCVPN)	1283
ADVPN	1310
Other VPN topics	1341
VPN IPsec troubleshooting	1363
SSL VPN	1370
SSL VPN best practices	1370
SSL VPN quick start	1373
SSL VPN tunnel mode	1380
SSL VPN web mode for remote user	1386
SSL VPN authentication	1391

SSL VPN to IPsec VPN	1469
SSL VPN protocols	1479
SSL VPN troubleshooting	1480
User & Device	1484
Endpoint control and compliance	1484
Per-policy disclaimer messages	1484
Compliance	1486
FortiGuard distribution of updated Apple certificates	1493
User Definition	1494
User types	1494
Removing a user	1494
User Groups	1495
Configuring POP3 authentication	1495
Dynamic policies - FortiClient EMS	1496
Guest Management	1502
Configuring guest access	1502
Retail environment guest access	1504
Device Inventory	1506
Device summary and filtering	1506
Adding MAC-based addresses to devices	1508
LDAP Servers	1510
FSSO polling connector agent installation	1510
Enabling Active Directory recursive search	1516
Configuring LDAP dial-in using a member attribute	1517
Configuring wildcard admin accounts	1518
Configuring least privileges for LDAP admin account authentication in Active Directory	1520
RADIUS Servers	1520
Configuring RADIUS SSO authentication	1520
RSA ACE (SecurID) servers	1526
TACACS+ Servers	1531
Authentication Settings	1532
FortiTokens	1534
FortiToken Mobile Quick Start Guide	1535
FortiToken Cloud	1546
Registering hard tokens	1547
Managing FortiTokens	1549
FortiToken Mobile Push	1551
Troubleshooting and diagnosis	1553
Configuring the maximum log in attempts and lockout period	1556
Creating a PKI/peer user	1557
Configuring firewall authentication	1557
Creating a locally authenticated user account	1558
Creating a RADIUS-authenticated user account	1558
Creating an FSSO user group	1559
Creating a firewall user group	1562
Defining policy addresses	1562

Creating security policies	1563
Wireless configuration	1565
Switch Controller	1566
FortiLink setup	1566
FortiLink auto network configuration policy	1567
FortiLink network sniffer extension	1568
FortiLink MCLAG configuration	1570
Standalone FortiGate as switch controller	1572
Standalone FortiGate as switch controller	1572
Multiple FortiSwitches managed via hardware/software switch	1575
Multiple FortiSwitches in tiers via aggregate interface with redundant link enabled	1579
Multiple FortiSwitches in tiers via aggregate interface with MCLAG enabled only on distribution	1582
HA (A-P) mode FortiGate pairs as switch controller	1586
Multiple FortiSwitches managed via hardware/software switch	1586
Multiple FortiSwitches in tiers via aggregate interface with redundant link enabled	1590
Multiple FortiSwitches in tiers via aggregate interface with MCLAG enabled on all tiers	1594
Authentication and security	1598
MAC-based 802.1X authentication	1598
Port-based 802.1X authentication	1601
MAC layer control - Sticky MAC and MAC Learning-limit	1604
Quarantine	1606
Flow and Device Detection	1607
Data statistic	1607
Security Fabric showing	1608
FortiSwitch multi-tenant support	1609
Persistent MAC learning	1612
Split port mode (for QSFP / QSFP28)	1613
Dynamic VLAN name assignment from RADIUS attribute	1614
MSTI support	1615
Netflow and IPFIX support	1616
Log and Report	1618
Viewing event logs	1618
Sample logs by log type	1619
Checking the email filter log	1639
Supported log types to FortiAnalyzer, FortiAnalyzer Cloud, FortiGate Cloud, and syslog	1640
Configuring multiple FortiAnalyzers on a multi-VDOM FortiGate	1640
Checking FortiAnalyzer connectivity	1642
Configuring multiple FortiAnalyzers (or syslog servers) per VDOM	1643
Source and destination UUID logging	1644
Troubleshooting	1646
Log-related diagnose commands	1646
Backing up log files or dumping log messages	1652
SNMP OID for logs that failed to send	1654

Monitor	1658
Policy and route checks	1658
WiFi client monitor	1660
WiFi health monitor	1661
Running processes	1662
Aggregate processes information	1664
VM	1667
Amazon Web Services	1667
Microsoft Azure	1667
Google Cloud Platform	1667
Oracle OCI	1667
AliCloud	1667
Private cloud	1667
FortiGate multiple connector support	1667
Adding VDOMs with FortiGate v-series	1670
Terraform: FortiOS as a provider	1673
Troubleshooting	1677
PF SR-IOV driver support	1678
Troubleshooting	1680
Troubleshooting methodologies	1680
Verify user permissions	1681
Establish a baseline	1681
Create a troubleshooting plan	1683
Troubleshooting scenarios	1684
Checking the system date and time	1685
Checking the hardware connections	1686
Checking FortiOS network settings	1687
Troubleshooting CPU and network resources	1690
Troubleshooting high CPU usage	1691
Checking the modem status	1695
Running ping and traceroute	1696
Checking the logs	1700
Verifying routing table contents in NAT mode	1700
Verifying the correct route is being used	1701
Verifying the correct firewall policy is being used	1701
Checking the bridging information in transparent mode	1702
Checking wireless information	1703
Performing a sniffer trace (CLI and packet capture)	1704
Debugging the packet flow	1707
Testing a proxy operation	1710
Displaying detail Hardware NIC information	1710
Performing a traffic trace	1713
Using a session table	1714
Finding object dependencies	1717
Diagnosing NPU-based interfaces	1718
Running the TAC report	1719
Other commands	1719

FortiGuard troubleshooting	1722
Additional resources	1725
Technical documentation	1725
Fortinet video library	1725
Release notes	1726
Knowledge base	1726
Fortinet technical discussion forums	1726
Fortinet training services online campus	1726
Fortinet Support	1726

Change Log

Date	Change Description
2023-06-08	Initial release.

Getting started

This section explains how to get started with a FortiGate.

Differences between models

Not all FortiGates have the same features, particularly entry-level models (models 30 to 90). A number of features on these models are only available in the CLI.



Consult your model's QuickStart Guide, [hardware manual](#), or the [Feature / Platform Matrix](#) for further information about features that vary by model.

FortiGate models differ principally by the names used and the features available:

- Naming conventions may vary between FortiGate models. For example, on some models the hardware switch interface used for the local area network is called *lan*, while on other units it is called *internal*.
- Certain features are not available on all models. Additionally, a particular feature may be available only through the CLI on some models, while that same feature may be viewed in the GUI on other models.

If you believe your FortiGate model supports a feature that does not appear in the GUI, go to *System > Feature Visibility* and confirm that the feature is enabled. For more information, see [Feature visibility on page 732](#).

Using the GUI

This section presents an introduction to the graphical user interface (GUI) on your FortiGate.

The following topics are included in this section:

- [Connecting using a web browser](#)
- [Menus](#)
- [Tables](#)
- [Entering values](#)

For information about using the dashboards, see [Dashboard on page 58](#).

Connecting using a web browser

In order to connect to the GUI using a web browser, an interface must be configured to allow administrative access over HTTPS or over both HTTPS and HTTP. By default, an interface has already been set up that allows HTTPS access with the IP address 192.168.1.99.

Browse to <https://192.168.1.99> and enter your username and password. If you have not changed the admin account's password, use the default user name, `admin`, and leave the password field blank.

The GUI will now be displayed in your browser.

To use a different interface to access the GUI:

1. Go to *Network > Interfaces* and edit the interface you wish to use for access. Take note of its assigned IP address.
2. Beside *Administrative Access*, select *HTTPS*, and any other protocol you require. You can also select *HTTP*, although this is not recommended as the connection will be less secure.
3. Click *OK*.
4. Browse to the IP address using your chosen protocol.
The GUI will now be displayed in your browser.

Menus



If you believe your FortiGate model supports a menu that does not appear in the GUI, go to *System > Feature Visibility* and ensure the feature is enabled. For more information, see [Feature visibility on page 732](#).

The GUI contains the following main menus, which provide access to configuration options for most FortiOS features:

Dashboard	The dashboard displays various widgets that display important system information and allow you to configure some system options. For more information, see Dashboard on page 58 .
Security Fabric	Access the physical topology, logical topology, automation, and settings of the Fortinet Security Fabric. For more information, see Fortinet Security Fabric on page 67 .
FortiView	A collection of dashboards and logs that give insight into network traffic, showing which users are creating the most traffic, what sort of traffic it is, when the traffic occurs, and what kind of threat the traffic may pose to the network. For more information, see FortiView on page 276 .
Network	Options for networking, including configuring system interfaces and routing options. For more information, see Network on page 315 .
System	Configure system settings, such as administrators, FortiGuard, and certificates. For more information, see System on page 617 .
Policy & Objects	Configure firewall policies, protocol options, and supporting content for policies, including schedules, firewall addresses, and traffic shapers. For more information, see Policy and Objects on page 767 .
Security Profiles	Configure your FortiGate's security features, including Antivirus, Web Filter, and Application Control. For more information, see Security Profiles on page 907 .
VPN	Configure options for IPsec and SSL virtual private networks (VPNs).

	For more information, see IPsec VPNs on page 1114 and SSL VPN on page 1370 .
User & Device	Configure user accounts, groups, and authentication methods, including external authentication and single sign-on (SSO).
WiFi & Switch Controller	Configure the unit to act as a wireless network controller, managing the wireless Access Point (AP) functionality of FortiWiFi and FortiAP units. On certain FortiGate models, this menu has additional features allowing for FortiSwitch units to be managed by the FortiGate. For more information, see Wireless configuration on page 1565 and Switch Controller on page 1566 .
Log & Report	Configure logging and alert email as well as reports. For more information, see Log and Report on page 1618 .
Monitor	View a variety of monitors, including the Routing Monitor, VPN monitors for both IPsec and SSL, monitors relating to wireless networking, and more.

Tables

Many GUI pages contain tables of information that can be filtered and customized to display specific information in a specific way. Some tables allow content to be edited directly on that table, or rows to be copied and pasted.

Navigation

Some tables contain information and lists that span multiple pages. Navigation controls will be available at the bottom of the page.

Filters

Filters are used to locate a specific set of information or content in a table. They can be particularly useful for locating specific log entries. The filtering options vary, depending on the type of information in the log.

Depending on the table content, filters can be applied using the filter bar, using a column filter, or based on a cell's content. Some tables allow filtering based on regular expressions.

Administrators with read and write access can define filters. Multiple filters can be applied at one time.

To manually create a filter:

1. Click *Add Filter* at the top of the table. A list of the fields available for filtering is shown.
2. Select the field to filter by.
3. Enter the value to filter by, adding modifiers as needed.
4. Press *Enter* to apply the filter.

To create a column filter:

1. Click the filter icon on the right side of the column header
2. Choose a filter type from the available options.
3. Enter the filter text, or select from the available values.
4. Click *Apply*.

To create a filter based on a cell's content:

1. Right click on a cell in the table.
2. Select a filtering option from the menu.

Column settings

Columns can be rearranged, resized, and added or removed from tables.

To add or remove columns:

1. Right a column header, or click the gear icon on the left side of the header row that appears when hovering the cursor over the headers.
2. Select columns to add or remove.
3. Click *Apply*.

To rearrange the columns in a table:

1. Click and drag the column header.

To resize a column:

1. Click and drag the right border of the column header.

To resize a column to fit its contents:

1. Click the dots or filter icon on the right side of the column header and select *Resize to Contents*.

To resize all of the columns in a table to fit their content:

1. Right a column header, or click the gear icon on the left side of the header row that appears when hovering the cursor over the headers.
2. Click *Best Fit All Columns*.

To reset a table to its default view:

1. Right a column header, or click the gear icon on the left side of the header row that appears when hovering the cursor over the headers.
2. Click *Reset Table*.
Resetting a table does not remove filters.

Editing objects

In some tables, parts of a configuration can be edited directly in the table. For example, security profiles can be added to an existing firewall policy by clicking the edit icon in a cell in the *Security Profiles* column.

Copying rows

In some tables, rows can be copied and pasted using the right-click menu. For example, a policy can be duplicated by copying and pasting it.

Entering values

Numerous fields in the GUI and CLI require text strings or numbers to be entered when configuring the FortiGate. When entering values in the GUI, you will be prevented from entering invalid characters, and a warning message will be shown explaining what values are not allowed. If invalid values are entered in a CLI command, the setting will be rejected when you apply it.

- [Text strings on page 21](#)
- [Numbers on page 22](#)

Text strings

Text strings are used to name entities in the FortiGate configuration. For example, the name of a firewall address, administrator, or interface are all text strings.

The following characters cannot be used in text strings, as they present cross-site scripting (XSS) vulnerabilities:

- " - double quotes
- ' - single quote
- > - greater than
- < - less than

Most GUI text fields prevent XSS vulnerable characters from being added.



VDOM names and hostnames can only use numbers (0-9), letters (a-z and A-Z), dashes, and underscores.

The `tree` CLI command can be used to view the number of characters allowed in a name field. For example, entering the following commands show that a firewall address name can contain up to 80 characters, while its FQDN can contain 256 characters:

```
config fire address
(address) # tree
-- [address] --*name      (80)
    |- uuid
    |- subnet
    |- type
    |- start-mac
    |- end-mac
```

```
| - start-ip
| - end-ip
| - fqdn      (256)
| - country   (3)
| - wildcard-fqdn (256)
| - cache-ttl  (0,86400)
| - wildcard
| - sdn        (36)
| - interface  (36)
| - tenant     (36)
| - organization (36)
| - epg-name    (256)
| - subnet-name (256)
| - sdn-tag     (16)
| - policy-group (16)
| - comment
| - visibility
| - associated-interface (36)
| - color       (0,32)
| - filter
| - sdn-addr-type
| - obj-id
| - [list] --*ip (36)
      | - obj-id (128)
      +- net-id (128)
| - [tagging] --*name (64)
      | - category (64)
      +- [tags] --*name (80)
+- allow-routing
```

Numbers

Numbers are used to set sizes, rates, addresses, port numbers, priorities, and other such numeric values. They can be entered as a series of digits (without commas or spaces), in a dotted decimal format (such as IP addresses), or separated by colons (such as MAC addresses). Most numeric values use base 10 numbers, while some use hexadecimal values.

Most GUI and CLI fields prevent invalid numbers from being entered. The CLI help text includes information about the range of values allowed for applicable settings.

Using the CLI

The Command Line Interface (CLI) can be used in lieu of the GUI to configure the FortiGate. Some settings are not available in the GUI, and can only be accessed using the CLI.

This section briefly explains basic CLI usage. For more information about the CLI, see the [FortiOS CLI Reference](#).

- [Connecting to the CLI on page 23](#)
- [CLI basics on page 25](#)
- [Command syntax on page 31](#)
- [Subcommands on page 34](#)
- [Permissions on page 36](#)

Connecting to the CLI

You can connect to the CLI using a direct console connection, SSH, the CLI console in the GUI, or the FortiExplorer app on your iOS device.

You can access the CLI outside of the GUI in three ways:

- **Console connection:** Connect your computer directly to the console port of your FortiGate.
- **SSH access:** Connect your computer through any network interface attached to one of the network ports on your FortiGate.
- **FortiExplorer:** Connect your device to the FortiExplorer app on your iOS device to configure, manage, and monitor your FortiGate. See [FortiExplorer for iOS on page 36](#) for details.

Console connection

A direct console connections to the CLI is created by directly connecting your management computer or console to the FortiGate unit, using its DB-9 or RJ-45 console port.

Direct console access to the FortiGate may be required if:

- You are installing the FortiGate for the first time and it is not configured to connect to your network.
- You are restoring the firmware using a boot interrupt. Network access to the CLI will not be available until after the boot process has completed, making direct console access the only option.

To connect to the FortiGate console, you need:

- A console cable to connect the console port on the FortiGate to a communications port on the computer. Depending on your device, this is one of:
 - null modem cable (DB-9 to DB-9)
 - DB-9 to RJ-45 cable (a DB-9-to-USB adapter can be used)
 - USB to RJ-45 cable
- A computer with an available communications port
- Terminal emulation software

To connect to the CLI using a direct console connection:

1. Using the console cable, connect the FortiGate unit's console port to the serial communications (COM) port on your management computer.
2. Start a terminal emulation program on the management computer, select the COM port, and use the following settings:

Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

3. Press Enter on the keyboard to connect to the CLI.
4. Log in to the CLI using your username and password (default: *admin* and no password).
You can now enter CLI commands, including configuring access to the CLI through SSH.

SSH access

SSH access to the CLI is accomplished by connecting your computer to the FortiGate unit using one of its network ports. You can either connect directly, using a peer connection between the two, or through any intermediary network.



If you do not want to use an SSH client and you have access to the GUI, you can access the CLI through the network using the CLI console in the GUI.

The CLI console can be accessed from the upper-right hand corner of the screen and appears as a slide-out window. For policies and objects, the CLI can be also be accessed by right clicking on the element and selecting *Edit in CLI*.

SSH must be enabled on the network interface that is associated with the physical network port that is used.

If your computer is not connected either directly or through a switch to the FortiGate, you must also configure the FortiGate with a static route to a router that can forward packets from the FortiGate to the computer. This can be done using a local console connection, or in the GUI.

To connect to the FortiGate CLI using SSH, you need:

- A computer with an available serial communications (COM) port and RJ-45 port
- The console cable
- Terminal emulation software
- A network cable
- Prior configuration of the operating mode, network interface, and static route.

To enable SSH access to the CLI using a local console connection:

1. Using the network cable, connect the FortiGate unit's port either directly to your computer's network port, or to a network through which your computer can reach the FortiGate unit.
2. Note the number of the physical network port.
3. Using direct console connection, connect and log into the CLI.
4. Enter the following command:

```
config system interface
  edit <interface_str>
    append allowaccess ssh
  next
end
```

Where `<interface_str>` is the name of the network interface associated with the physical network port, such as `port1`.

5. Confirm the configuration using the following command to show the interface's settings:

```
show system interface <interface_str>
```

For example:

```
show system interface port1
config system interface
  edit "port1"
    set vdom "root"
    set ip 192.168.1.99 255.255.255.0
    set allowaccess ping https ssh
    set type hard-switch
```

```
        set stp enable
        set role lan
        set snmp-index 6
    next
end
```

Connecting using SSH

Once the FortiGate unit is configured to accept SSH connections, use an SSH client on your management computer to connect to the CLI.

The following instructions use [PuTTY](#). The steps may vary in other terminal emulators.

To connect to the CLI using SSH:

1. On your management computer, start PuTTY.
2. In the *Host Name (or IP address)* field, enter the IP address of the network interface that you are connected to and that has SSH access enabled.
3. Set the port number to 22, if it is not set automatically.
4. Select *SSH* for the *Connection type*.
5. Click *Open*. The SSH client connects to the FortiGate.
The SSH client may display a warning if this is the first time that you are connecting to the FortiGate and its SSH key is not yet recognized by the SSH client, or if you previously connected to the FortiGate using a different IP address or SSH key. This is normal if the management computer is connected directly to the FortiGate with no network hosts in between.
6. Click *Yes* to accept the FortiGate unit's SSH key.
The CLI displays the log in prompt.
7. Enter a valid administrator account name, such as `admin`, then press *Enter*.
8. Enter the administrator account password, then press *Enter*.
The CLI console shows the command prompt (FortiGate hostname followed by a #). You can now enter CLI commands.



If three incorrect log in or password attempts occur in a row, you will be disconnected. If this occurs, wait for one minute, then reconnect and attempt to log in again.

CLI basics

Basic features and characteristics of the CLI environment provide support and ease of use for many CLI tasks.

Help

Press the question mark (?) key to display command help and complete commands.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.
- Enter a command followed by a space and press the question mark (?) key to display a list of the options available for that command and a description of each option.

- Enter a command followed by an option and press the question mark (?) key to display a list of additional options available for that command option combination and a description of each option.
- Enter a question mark after entering a portion of a command to see a list of valid complete commands and their descriptions. If there is only one valid command, it will be automatically filled in.

Shortcuts and key commands

Shortcut key	Action
?	List valid complete or subsequent commands. If multiple commands can complete the command, they are listed with their descriptions.
Tab	Complete the word with the next available match. Press multiple times to cycle through available matches.
Up arrow or Ctrl + P	Recall the previous command. Command memory is limited to the current session.
Down arrow, or Ctrl + N	Recall the next command.
Left or Right arrow	Move the cursor left or right within the command line.
Ctrl + A	Move the cursor to the beginning of the command line.
Ctrl + E	Move the cursor to the end of the command line.
Ctrl + B	Move the cursor backwards one word.
Ctrl + F	Move the cursor forwards one word.
Ctrl + D	Delete the current character.
Ctrl + C	Abort current interactive commands, such as when entering multiple lines. If you are not currently within an interactive command such as <code>config</code> or <code>edit</code> , this closes the CLI connection.
\ then Enter	Continue typing a command on the next line for a multiline command. For each line that you want to continue, terminate it with a backslash (\). To complete the command, enter a space instead of a backslash, and then press <i>Enter</i> .

Command tree

Enter `tree` to display the CLI command tree. To capture the full output, connect to your device using a terminal emulation program and capture the output to a log file. For some commands, use the `tree` command to view all available variables and subcommands.

Command abbreviation

You can abbreviate words in the command line to their smallest number of non-ambiguous characters.

For example, the command `get system status` could be abbreviated to `g sy stat`.

Adding and removing options from lists

When configuring a list, the `set` command will remove the previous configuration.

For example, if a user group currently includes members A, B, and C, the command `set member D` will remove members A, B, and C. To avoid removing the existing members from the group, the command `set members A B C D` must be used.

To avoid this issue, the following commands are available:

append	Add an option to an existing list. For example, <code>append member D</code> adds user D to the user group without removing any of the existing members.
select	Clear all of the options except for those specified. For example, <code>select member B</code> removes all member from the group except for member B.
unselect	Remove an option from an existing list. For example, <code>unselect member C</code> removes only member C from the group, without affecting the other members.

Environment variables

The following environment variables are support by the CLI. Variable names are case-sensitive.

\$USERFROM	The management access type (<code>ssh</code> , <code>jsconsole</code> , and so on) and the IPv4 address of the administrator that configured the item.
\$USERNAME	The account name of the administrator that configured the item.
\$SerialNum	The serial number of the FortiGate unit.

For example, to set a FortiGate device's host name to its serial number, use the following CLI command:

```
config system global
    set hostname $SerialNum
end
```

Special characters

The following characters cannot be used in most CLI commands: `<`, `>`, `(`, `)`, `#`, `'`, and `"`

If one of those characters, or a space, needs to be entered as part of a string, it can be entered by using a special command, enclosing the entire string in quotes, or preceding it with an escape character (backslash, `\`).

To enter a question mark (`?`) or a tab, `Ctrl + V` must be entered first.



Question marks and tabs cannot be typed or copied into the CLI Console or some SSH clients.

Character	Keys
?	Ctrl + V then ?
Tab	Ctrl + V then Tab
Space (as part of a string value, not to end the string)	Enclose the string in single or double quotation marks: "Security Administrator". or 'Security Administrator'. Precede the space with a backslash: Security\ Administrator.
' (as part of a string value, not to begin or end the string)	\'
" (as part of a string value, not to begin or end the string)	\"
\	\\

Using grep to filter command output

The `get`, `show`, and `diagnose` commands can produce large amounts of output. The `grep` command can be used to filter the output so that it only shows the required information.

The `grep` command is based on the standard UNIX `grep`, used for searching text output based on regular expressions.

For example, the following command displays the MAC address of the internal interface:

```
get hardware nic internal | grep Current_HWaddr
Current_HWaddr          00:09:0f:cb:c2:75
```

The following command will display all TCP sessions that are in the session list, including the session list line number in the output:

```
get system session list | grep -n tcp
```

The following command will display all of the lines in the HTTP replacement message that contain URL or url:

```
show system replacemsg http | grep -i url
```

The following options can also be used:

```
-A <num> After
-B <num> Before
-C <num> Context
```

The `-f` option is available to support contextual output, in order to show the complete configuration. The following example shows the difference in the output when `-f` is used versus when it is not used:

Without `-f`:

```
show | grep ldap-group1
edit "ldap-group1"
set groups "ldap-group1"
```

With `-f`:

```
show | grep -f ldap-group1
config user group
edit "ldap-group1"
set member "pc40-LDAP"
next
```

```
end
config firewall policy
    edit 2
        set srcintf "port31"
        set dstintf "port32"
        set srcaddr "all"
        set action accept
        set identity-based enable
        set nat enable
        config identity-based-policy
            edit 1
                set schedule "always"
                set groups "ldap-group1"
                set dstaddr "all"
                set service "ALL"
            next
        end
    next
end
```

Language support and regular expressions

Characters such as ñ and é, symbols, and ideographs are sometimes acceptable input. Support varies depending on the type of item that is being configured. CLI commands, objects, field names, and options must use their exact ASCII characters, but some items with arbitrary names or values can be input using your language of choice. To use other languages in those cases, the correct encoding must be used.

Input is stored using Unicode UTF-8 encoding, but is not normalized from other encodings into UTF-8 before it is stored. If your input method encodes some characters differently than in UTF-8, configured items may not display or operate as expected.

Regular expressions are especially impacted. Matching uses the UTF-8 character values. If you enter a regular expression using a different encoding, or if an HTTP client sends a request in a different encoding, matches may not be what is expected.

For example, with Shift-JIS, backslashes could be inadvertently interpreted as the symbol for the Japanese yen (¥), and vice versa. A regular expression intended to match HTTP requests containing monetary values with a yen symbol may not work if the symbol is entered using the wrong encoding.

For best results:

- use UTF-8 encoding, or
- use only characters whose numerically encoded values are the same in UTF-8, such as the US-ASCII characters that are encoded using the same values in ISO 8859-1, Windows code page 1252, Shift-JIS, and other encoding methods, or
- for regular expressions that must match HTTP requests, use the same encoding as your HTTP clients.



HTTP clients may send requests in encodings other than UTF-8. Encodings usually vary based on the client's operating system or input language. If the client's encoding method cannot be predicted, you might only be able to match the parts of the request that are in English, as the values for English characters tend to be encoded identically, regardless of the encoding method.

If the FortiGate is configured to use an encoding method other than UTF-8, the management computer's language may need to be changed, including the web browser and terminal emulator. If the FortiGate is configured using non-ASCII characters, all the systems that interact with the FortiGate must also support the same encoding method. If possible, the same encoding method should be used throughout the configuration to avoid needing to change the language settings on the management computer.

The GUI and CLI client normally interpret output as encoded using UTF-8. If they do not, configured items may not display correctly. Exceptions include items such as regular expression that may be configured using other encodings to match the encoding of HTTP requests that the FortiGate receives.

To enter non-ASCII characters in a terminal emulator:

1. On the management computer, start the terminal client.
2. Configure the client to send and receive characters using UTF-8 encoding.
Support for sending and receiving international characters varies by terminal client.
3. Log in to the FortiGate unit.
4. At the command prompt, type your command and press *Enter*.
Words that use encoded characters may need to be enclosed in single quotes (').
Depending on your terminal client's language support, you may need to interpret the characters into character codes before pressing *Enter*. For example, you might need to enter: `edit '\743\601\613\743\601\652 '`
5. The CLI displays the command and its output.

Screen paging

By default, the CLI will pause after displaying each page worth of text when a command has multiple pages of output. This can be useful when viewing lengthy outputs that might exceed the buffer of terminal emulator.

When the display pauses and shows `--More--`, you can:

- Press *Enter* to show the next line,
- Press *Q* to stop showing results and return to the command prompt,
- Press an arrow key, *Insert*, *Home*, *Delete*, *End*, *Page Up*, or *Page Down* to show the next few pages,
- Press any other key to show the next page, or
- Wait for about 30 seconds for the console to truncate the output and return to the command prompt.

When pausing the screen is disabled, press *Ctrl* + *C* to stop the output and log out of the FortiGate.

To disable pausing the CLI output:

```
config system console
    set output standard
end
```

To enable pausing the CLI output:

```
config system console
    set output more
end
```

Changing the baud rate

The baud rate of the local console connection can be changed from its default value of 9600.

To change the baud rate:

```
config system console
  set baudrate {9600 | 19200 | 38400 | 57600 | 115200}
end
```

Editing the configuration file

The FortiGate configuration file can be edited on an external host by backing up the configuration, editing the configuration file, and then restoring the configuration to the FortiGate.

Editing the configuration file can save time if many changes need to be made, particularly if the plain text editor that you are using provides features such as batch changes.

To edit the configuration file:

1. Backup the configuration. See [Configuration backups on page 62](#) for details.
2. Open the configuration file in a plain text editor that supports UNIX-style line endings.
3. Edit the file as needed.



Do not edit the first line of the configuration file.

This line contains information about the firmware version and FortiGate model. If you change the model number, the FortiGate unit will reject the configuration when you attempt to restore it.

4. Restore the modified configuration to the FortiGate. See [Configuration backups on page 62](#) for details.
The FortiGate downloads the configuration file and checks that the model information is correct. If it is correct, the configuration file is loaded and each line is checked for errors. If a command is invalid, that command is ignored. If the configuration file is valid, the FortiGate restarts and loads the downloaded configuration.

Command syntax

When entering a command, the CLI console requires that you use valid syntax and conform to expected input constraints. It rejects invalid commands. Indentation is used to indicate the levels of nested commands.

Each command line consists of a command word, usually followed by configuration data or a specific item that the command uses or affects.

Notation

Brackets, vertical bars, and spaces are used to denote valid syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

All syntax uses the following conventions:

Angle brackets < >	Indicate a variable of the specified data type.
Curly brackets { }	Indicate that a variable or variables are mandatory.
Square brackets []	Indicate that the variable or variables are optional. For example: <code>show system interface [<name_str>]</code> To show the settings for all interfaces, you can enter <code>show system interface</code> To show the settings for the Port1 interface, you can enter <code>show system interface port1</code> .
Vertical bar 	A vertical bar separates alternative, mutually exclusive options. For example: <code>set protocol {ftp sftp}</code> You can enter either <code>set protocol ftp</code> or <code>set protocol sftp</code> .
Space	A space separates non-mutually exclusive options. For example: <code>set allowaccess {ping https ssh snmp http fgfm radius-acct probe-response capwap ftm}</code> You can enter any of the following: <code>set allowaccess ping</code> <code>set allowaccess https ping ssh</code> <code>set allowaccess http https snmp ssh ping</code> In most cases, to make changes to lists that contain options separated by spaces, you need to retype the entire list, including all the options that you want to apply and excluding all the options that you want to remove.

Optional values and ranges

Any field that is optional will use square-brackets. The overall config command will still be valid whether or not the option is configured.

Square-brackets can be used to show that multiple options can be set, even intermixed with ranges. The following example shows a field that can be set to either a specific value or range, or multiple instances:

```
config firewall service custom
  set iprange <range1> [<range2> <range3> ...]
end
```

next

The `next` command is used to maintain a hierarchy and flow to CLI commands. It is at the same indentation level as the preceding `edit` command, to mark where a table entry finishes.

The following example shows the `next` command used in the subcommand `entries`:

```
config dlp filepattern
edit <1>
    set name <name>
    set comment [comment]
    config entries
        edit <2>
            set filter-type {pattern | type}
        next
    ←
```

After configuring table entry <2> then entering `next`, the <2> table entry is saved and the console returns to the `entries` prompt:

```
FGT60E1Q23456789 (entries) #
```

You can now create more table entries as needed, or enter `end` to save the table and return to the `filepattern` table element prompt.

end

The `end` command is used to maintain a hierarchy and flow to CLI commands.

The following example shows the same command and subcommand as the `next` command example, except `end` has been entered instead of `next` after the subcommand:

```
config dlp filepattern
edit <1>
    set name <name>
    set comment [comment]
    config entries
        edit <2>
            set filter-type {pattern | type}
        end
    ←
```

Entering `end` will save the <2> table entry and the table, and exit the `entries` subcommand entirely. The console returns to the `filepattern` table element prompt:

```
FGT60E1Q23456789 (1) #
```

Subcommands

Subcommands are available from within the scope of some commands. When you enter a subcommand level, the command prompt changes to indicate the name of the current command scope. For example, after entering:

```
config system admin
```

the command prompt becomes:

```
(admin)#
```

Applicable subcommands are available until you exit the command, or descend an additional level into another subcommand. Subcommand scope is indicated by indentation.

For example, the `edit` subcommand is only available in commands that affects tables, and the `next` subcommand is available only in the `edit` subcommand:

```
config system interface
  edit port1
    set status up
  next
end
```

The available subcommands vary by command. From a command prompt under the `config` command, subcommands that affect tables and fields could be available.

Table subcommands

edit <table_row>

Create or edit a table value.

In objects such as security policies, <table_row> is a sequence number. To create a new table entry without accidentally editing an existing entry, enter `edit 0`. The CLI will confirm that creation of entry 0, but will assign the next unused number when the entry is saved after entering `end` or `next`.

For example, to create a new firewall policy, enter the following commands:

```
config firewall policy
  edit 0
  ....
  next
end
```

To edit an existing policy, enter the following commands:

```
config firewall policy
  edit 27
  ....
  next
end
```

The `edit` subcommand changes the command prompt to the name of the table value that is being edited.

delete <table_row>

Delete a table value.

For example, to delete firewall policy 30, enter the following commands:

```
config firewall policy
  delete 30
end
```


purge	<p>Clear all table values.</p> <p>The <code>purge</code> command cannot be undone. To restore purged table values, the configuration must be restored from a backup.</p>
move	<p>Move an ordered table value.</p> <p>In the firewall policy table, this equivalent to dragging a policy into a new position. It does not change the policy's ID number.</p> <p>For example, to move policy 27 to policy 30, enter the following commands:</p> <pre>config firewall policy move 27 to 30 end</pre> <p>The <code>move</code> subcommand is only available in tables where the order of the table entries matters.</p>
clone <table_row> to <table_row>	<p>Make a clone of a table entry.</p> <p>For example, to create firewall policy 30 as a clone of policy 27, enter the following commands:</p> <pre>config firewall policy clone 27 to 30 end</pre> <p>The <code>clone</code> subcommand may not be available for all tables.</p>
rename <table_row> to <table_row>	<p>Rename a table entry.</p> <p>For example to rename an administrator from Flank to Frank, enter the following commands:</p> <pre>config system admin rename Flank to Frank end</pre> <p>The <code>rename</code> subcommand is only available in tables where the entries can be renamed.</p>
get	<p>List the current table entries.</p> <p>For example, to view the existing firewall policy table entries, enter the following commands:</p> <pre>config firewall policy get</pre>
show	<p>Show the configuration. Only table entries that are not set to default values are shown.</p>
end	<p>Save the configuration and exit the current <code>config</code> command.</p>



Purging the `system interface` or `system admin` tables does not reset default table values. This can result in being unable to connect to or log in to the FortiGate, requiring the FortiGate to be formatted and restored.

Field subcommands

set <field> <value>	Modify the value of a field.
--	------------------------------

	For example, the command <code>set fsso enable</code> sets the <code>fsso</code> field to the value <code>enable</code> .
unset	Set the field to its default value.
select	Clear all of the options except for those specified. For example, if a group contains members A, B, C, and D, to remove all members except for B, use the command <code>select member B</code> .
unselect	Remove an option from an existing list. For example, if a group contains members A, B, C, and D, to remove only member B, use the command <code>unselect member B</code> .
append	Add an option to an existing multi-option table value.
clear	Clear all the options from a multi-option table value.
get	List the configuration of the current table entry, including default and customized values.
show	Show the configuration. Only values that are not set to default values are shown.
next	Save changes to the table entry and exit the <code>edit</code> command so that you can configure the next table entry.
abort	Exit the command without saving.
end	Save the configuration and exit the current <code>config</code> command.

Permissions

Administrator, or access, profiles control what CLI commands an administrator can access by assigning read, write, or no access to each are of FortiOS. For information, see [Administrator profiles on page 619](#).

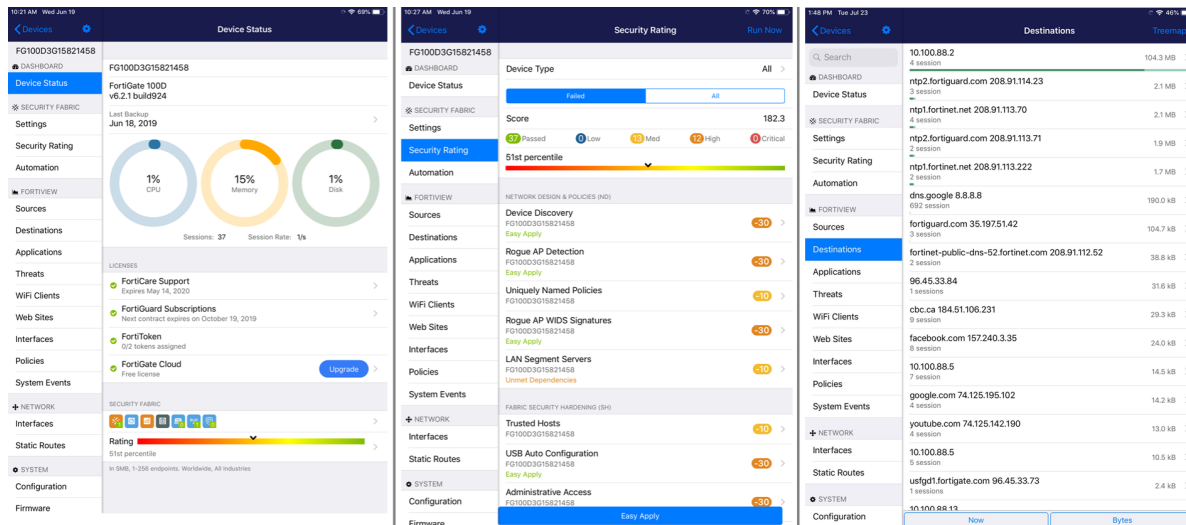
Read access is required to view configurations. Write access is required to make configuration changes. Depending on your account's profile, you may not have access to all CLI commands. To have access to all CLI commands, an administrator account with the *super_admin* profile must be used, such as the *admin* account.

Accounts assigned the *super_admin* profile are similar to the root administrator account. They have full permission to view and change all FortiGate configuration options, including viewing and changing other administrator accounts.

To increase account security, set strong passwords for all administrator accounts, and change the passwords regularly.

FortiExplorer for iOS

FortiExplorer for iOS is a user-friendly application that helps you to rapidly provision, deploy, and monitor Security Fabric components from your iOS device.



FortiExplorer for iOS requires iOS 10.0 or later and is compatible with iPhone, iPad, and Apple TV. It is supported by FortiOS 5.6 and later, and is only available on the [App Store](#) for iOS devices.

Advanced features are available with the purchase of FortiExplorer Pro. Paid features include the ability to add more than two devices and the ability to download firmware images from FortiCare.

Up to six members can use this app with 'Family Sharing' enabled in the App Store.



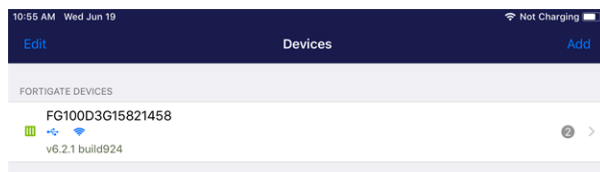
Firmware upload requires a valid firmware license. Users can download firmware for models with a valid support contract.

Getting started with FortiExplorer

If your FortiGate is accessible on a wireless network, you can connect to it using FortiExplorer provided that your iOS device is on the same network (see [Connecting FortiExplorer to a FortiGate via WiFi](#)). Otherwise, you will need to physically connect your iOS device to the FortiGate using a USB cable.

To connect and configure a FortiGate with FortiExplorer using a USB connection:

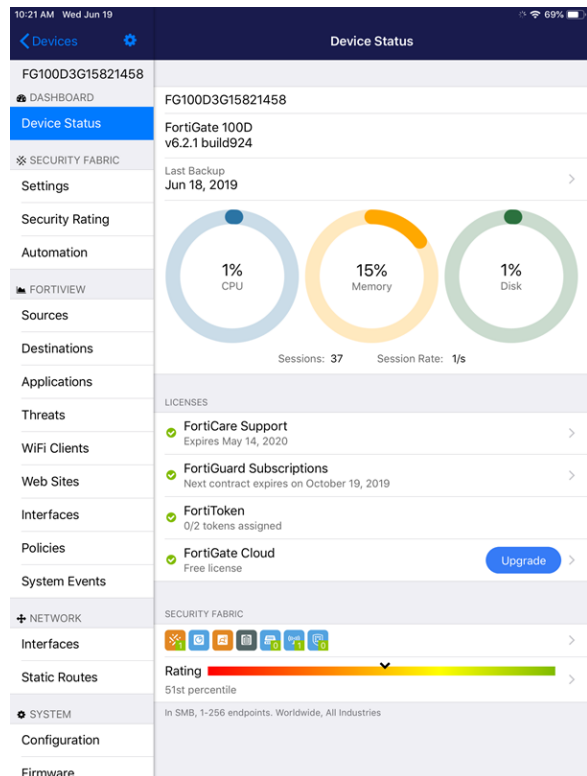
1. Connect your iOS device to your FortiGate USB A port. If prompted on your iOS device, *Trust* this computer.
2. Open FortiExplorer and select your FortiGate from the *FortiGate Devices* list. A blue USB icon will indicate that you are connected over a USB connection.



3. On the *Login* screen, select *USB*.
4. Enter the default *Username* (admin) and leave the *Password* field blank.
5. Optionally, select *Remember Password*.

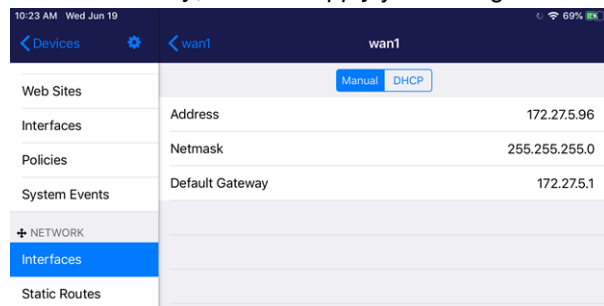
6. Tap *Done* when you are ready.

FortiExplorer opens the FortiGate management interface to the *Device Status* page:

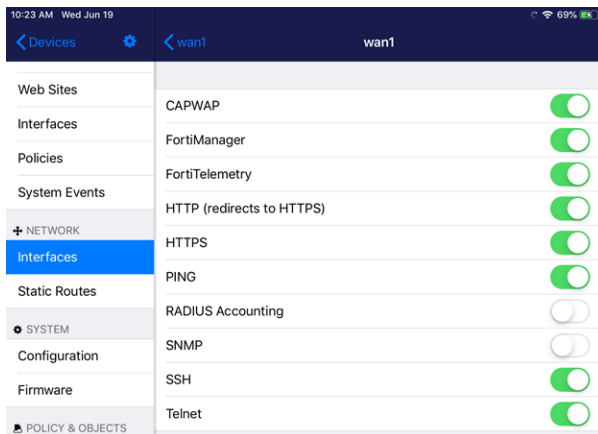


7. Go to *Network > Interfaces* and configure the WAN interface or interfaces.

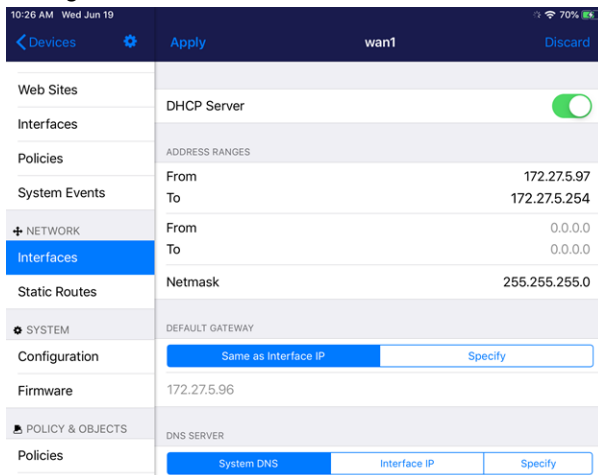
8. The *wan1* interface *Address mode* is set to *DHCP* by default. Set it to *Manual* and enter its *Address*, *Netmask*, and *Default Gateway*, and then *Apply* your changes.



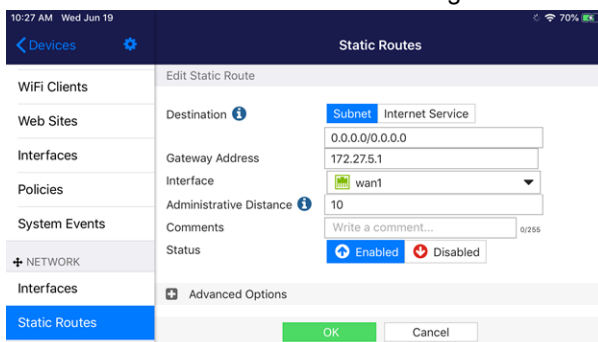
9. Optionally, configure *Administrative Access* to allow *HTTPS* access. This will allow administrators to access the FortiGate GUI using a web browser.



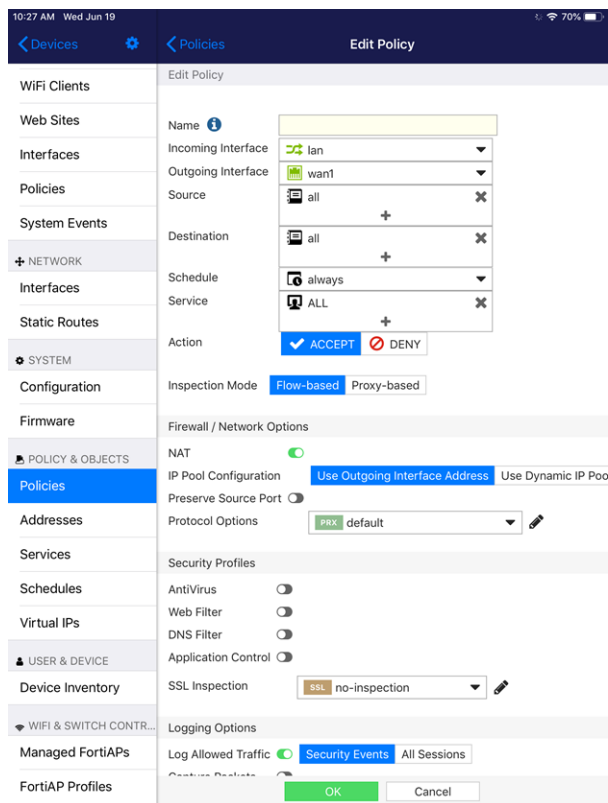
10. Go to *Network > Interfaces* and configure the local network (internal) interface.
11. Set the *Address* mode as before and configure *Administrative Access* if required.
12. Configure a *DHCP Server* for the internal network subnet.



13. Return to the internal interface using the < button at the top of the screen.
14. Go to *Network > Static Routes* and configure the static route to the gateway.



15. Go to *Policy & Objects > IPv4 Policy* and edit the Internet access policy. Enter a *Name* for the policy, enable the required *Security Profiles*, configure *Logging Options*, then tap *OK*.

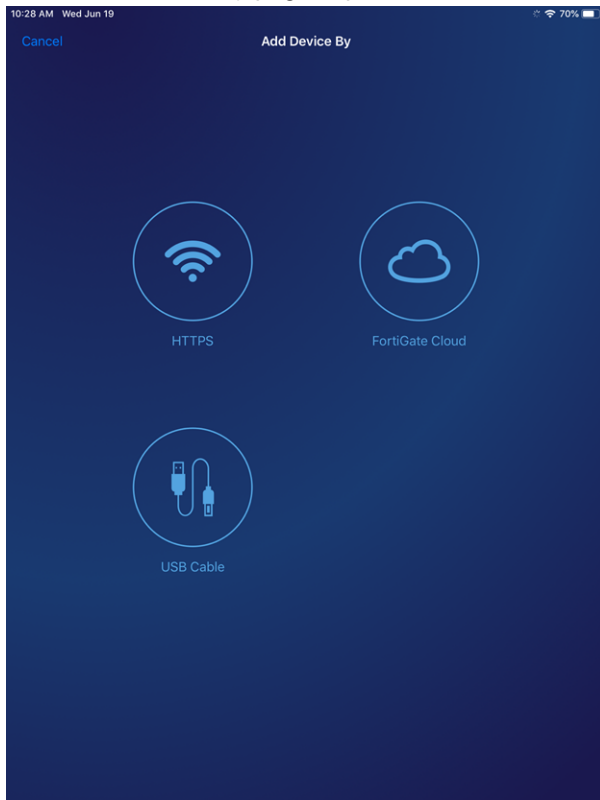


Connecting FortiExplorer to a FortiGate via WiFi

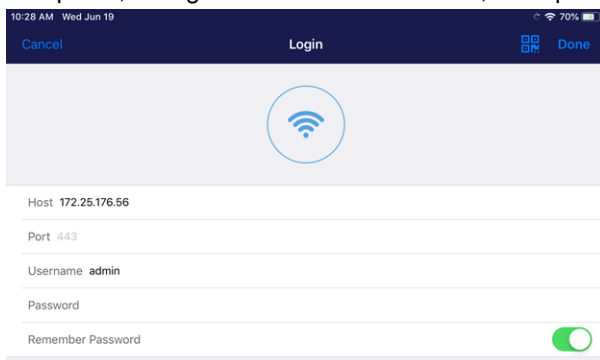
You can wirelessly connect to the FortiGate if your iOS device and the FortiGate are both connected to the same wireless network.

To connect and configure a FortiGate with FortiExplorer wirelessly:

1. Open the FortiExplorer app and tap *Add* on the *Devices* page.
2. On the *Add Device By* page, tap *HTTPS*.



3. Enter the *Host* information, *Username*, and *Password*.
4. If required, change the default *Port* number, and optionally enable *Remember Password*.

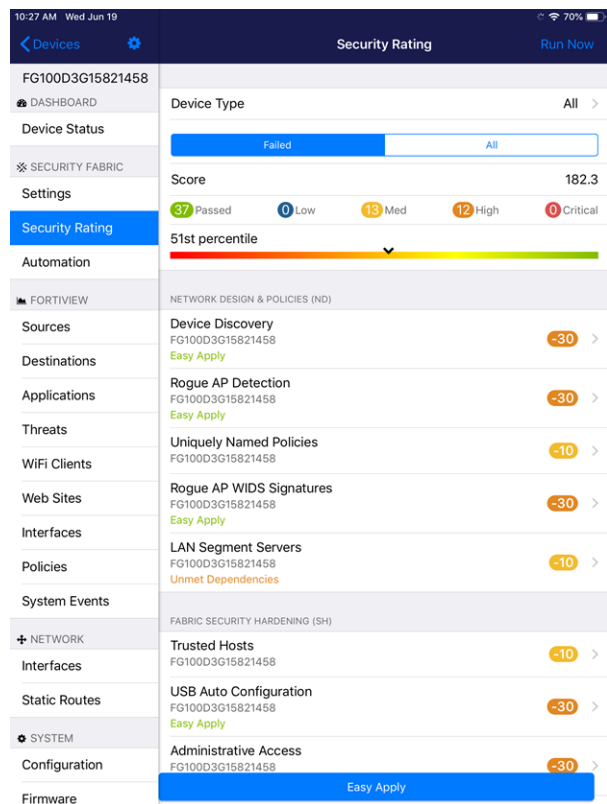


5. Tap *Done*.
6. If the FortiGate device identity cannot be verified, tap *Connect* at the prompt.
FortiExplorer opens the FortiGate management interface to the *Device Status* page.

Running a security rating

After configuring your network, run a security rating check to identify vulnerabilities and highlight best practices that could improve your network's security and performance.

Go to *Security Fabric > Security Rating* and follow the steps to determine the score. See [Security rating on page 133](#) for more information.



Upgrading to FortiExplorer Pro

FortiExplorer Pro includes the option to add more than two devices and download firmware images from FortiCare.

To upgrade to FortiExplorer Pro:

1. In FortiExplorer, go to *Settings*.
2. Tap *Upgrade to FortiExplorer Pro*.
3. Follow the on-screen prompts.

Basic administration

This section contains information about basic FortiGate administration that you can do after you installing the unit in your network.

- [Registration on page 43](#)
- [FortiCare and FortiGate Cloud login on page 46](#)

Registration

The FortiGate, and then its service contract, must be registered to have full access to [Fortinet Customer Service and Support](#), and [FortiGuard](#) services. The FortiGate can be registered in either the FortiGate GUI or the FortiCloud support portal. The service contract can be registered from the FortiCloud support portal.



The service contract number is needed to complete registrations on the FortiCloud support portal. You can find this 12-digit number in the email that contains your service registration document (sent from do-not-reply-contract@fortinet.com) in the service entitlement summary.

To register your FortiGate:

1. Connect to the FortiGate GUI. A message is shown stating that FortiCare registration is required.

The screenshot shows a dialog box titled "FortiCare Registration Required". Inside, there is a yellow warning box with a triangle icon and the text: "This step is required to activate threat protection services and receive firmware & package updates." Below this, there are two buttons: "Register Now" (highlighted in green) and "Later".

2. Click *Register Now*.
3. If you already have a support account, set *Action* to *Login*, and enter the required information.

The screenshot shows the "FortiCare Registration Required" dialog box with the following fields and options:

- Serial Number: *FG800D3915800295*
- Action: **Login** (highlighted in green) and *Create Account*
- Email:
- Password:
- Forgot your password?: [Forgot your password?](#)
- Country:
- Reseller:
- Buttons: **OK** (highlighted in green) and *Cancel*

If you need to create an account, set *Action* to *Create Account*, and enter the required information.

FortiCare Registration Required

Serial Number *FG800D3915800295*

Action

About You

First Name

Last Name

Title

Sign-In

Email

Password

Confirm Password

Contact

Company

Phone Number

Fax Number

Address

Address

City

Postal / Zip Code

Country

State / Province

4. Click **OK**.
5. Go to *System > FortiGuard*.
6. In the *License Information* table, the *FortiCare Support* status is *Registered*. There may be a delay before the status is updated on your FortiGate.

To register the FortiGate on the FortiCloud support portal:

1. Go to support.fortinet.com and log in using your FortiCloud account credentials. If you do not have an account, click *Register* to create one.
2. Click *Asset > Register/Activate*.

- Enter your product serial number or license certificate number for a VM, select an end user type, then click *Next*.

Registration Wizard | Registering Product

1 Registration Code > 2 > 3 > 4

Specify Registration Code
Please enter your product serial number, service contract registration code or license certificate number to start the registration:

End User Type
Please specify the type of user who will be using this product:

☐ The product will be used by a government user ☐ The product will be used by a non-government user

In this context a government end-user is any central, regional or local government department, agency, or other entity performing governmental functions; including (1) governmental research institutions, (2) governmental corporations or their separate business units which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List, and (3) international governmental organizations.

Next

- Enter your support contract number and product description, select a Fortinet partner, then click *Next*.
- Read through the service terms and conditions, select the checkbox to accept, then click *Next*.
- Verify the product entitlement preview, read through the terms and select the checkbox to accept, then click *Confirm*.
- The *Registration Completed* page appears where page you can download the license file. Click *Register More* to register another FortiGate, or click *Finish* to complete the registration process.

To register the service contract on the FortiCloud support portal:

- Go to support.fortinet.com and log in using your FortiCloud account credentials.
- Click *Asset > Register/Activate*.
- Enter your 12-digit contract registration code (service contract number), then click *Next*.
- Enter the device serial number or select it from the list, then click *Next*.
- Read through the service terms and conditions, select the checkbox to accept, then click *Next*.
- Verify the product entitlement preview and associated services, read through the terms and select the checkbox to accept, then click *Confirm*.
- Click *Asset > Manage/View Products*.
- Select the device, then click *Entitlement* in the left menu to view the service entitlement.

[Back To List](#)

Support Type	Support Level	Activation Date	Expiration Date
Hardware	Advanced HW	2020-03-05	2021-03-05
Firmware & General Updates	Web/Online	2020-03-05	2021-03-05
Enhanced Support	24x7	2020-03-05	2021-03-05
Telephone Support	24x7	2020-03-05	2021-03-05
Advanced Malware Protection	Web/Online	2020-03-05	2021-03-05
NGFW	Web/Online	2020-03-05	2021-03-05
Web Filtering	Web/Online	2020-03-05	2021-03-05
AntiSpam	Web/Online	2020-03-05	2021-03-05
FortiSandbox Cloud	Web/Online	2020-03-05	2021-03-05

FortiCare and FortiGate Cloud login

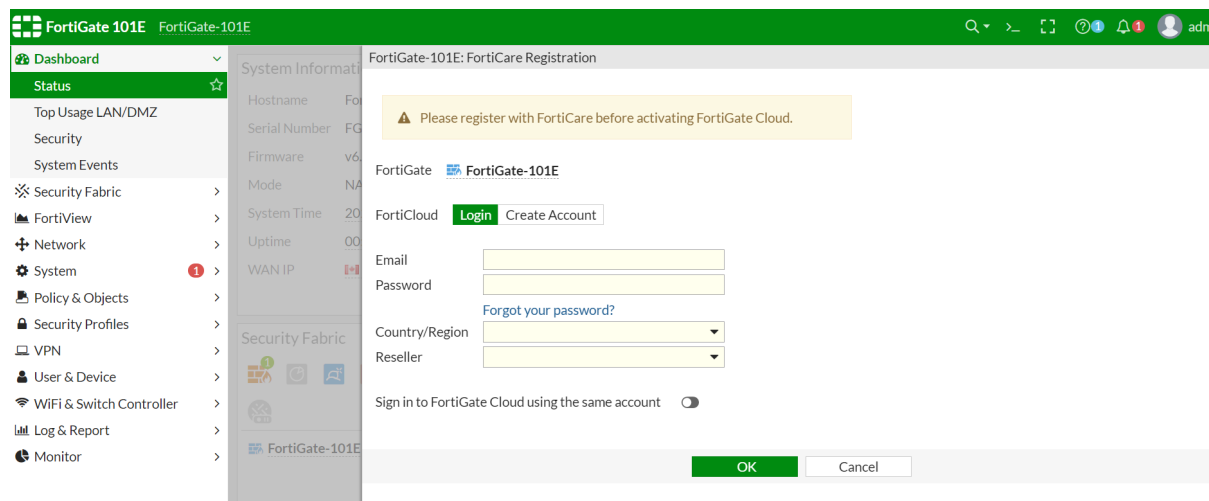
With FortiCloud, FortiGate supports a unified login to FortiCare and FortiGate Cloud. The FortiGate Cloud setup is a subset of the FortiCare setup.

- If the FortiGate is not registered, activating FortiGate Cloud will force you to register with FortiCare.
- If a FortiGate is registered in FortiCare using a FortiCloud account, then only that FortiCloud account can be used to activate FortiGate Cloud.
- If a different FortiCloud account was already used to activate FortiGate Cloud, then a notification asking you to migrate to FortiCloud is shown in the GUI after upgrading FortiOS.

The CLI can be used to activate FortiGate Cloud without registration, or with a different FortiCloud account.

To activate FortiGate Cloud and register with FortiCare at the same time:

1. Go to *Dashboard > Status*.
2. In the FortiGate Cloud widget, click *Not Activated > Activate*.
You must register with FortiCare before activating FortiGate Cloud.



The screenshot shows the FortiGate 101E FortiCare Registration dialog box. The dialog has a green header bar with the FortiGate logo and the text 'FortiGate-101E'. Below the header, there is a warning message: 'Please register with FortiCare before activating FortiGate Cloud.' The main content area contains the following fields and options:

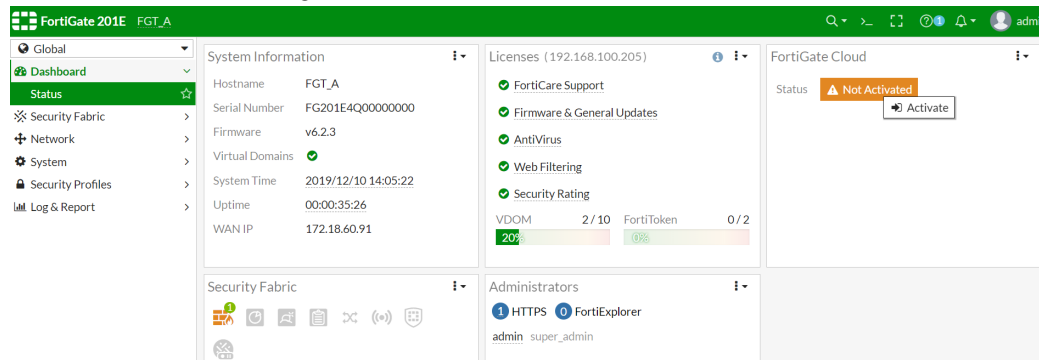
- FortiGate:** FortiGate-101E
- FortiCloud:** Login (selected) | Create Account
- Email:** [Text input field]
- Password:** [Text input field]
- Forgot your password?:** [Link]
- Country/Region:** [Dropdown menu]
- Reseller:** [Dropdown menu]
- Sign in to FortiGate Cloud using the same account:** [Toggle switch, currently off]

At the bottom of the dialog, there are two buttons: 'OK' (green) and 'Cancel' (white).

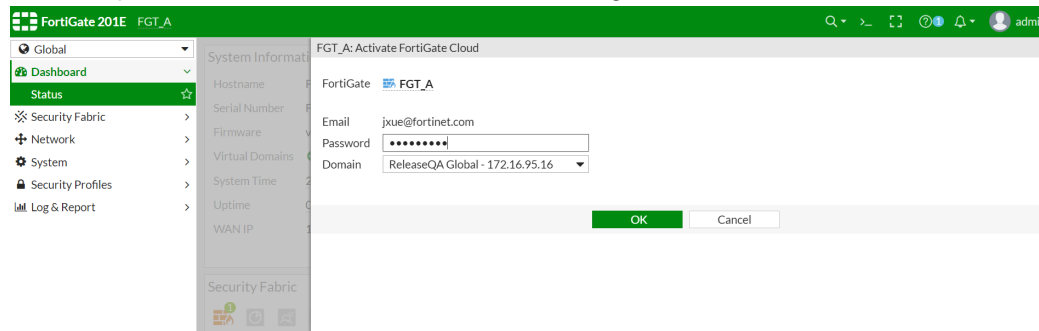
3. Enter your FortiCare *Email* address and *Password*.
4. Select your *Country/Region* and *Reseller*.
5. Enable *Sign in to FortiGate Cloud using the same account*.
6. Click **OK**.

To activate FortiGate Cloud on an already registered FortiGate:

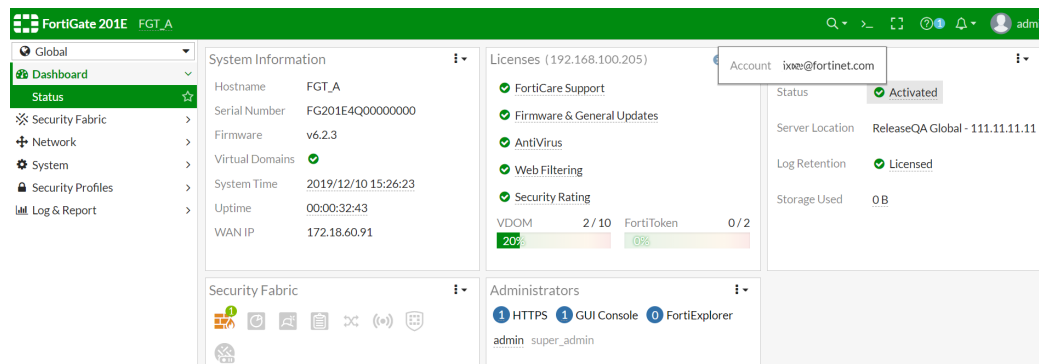
1. Go to *Dashboard > Status*.
2. In the FortiGate Cloud widget, click *Not Activated > Activate*.



3. Enter the password for the account that was used to register the FortiGate.

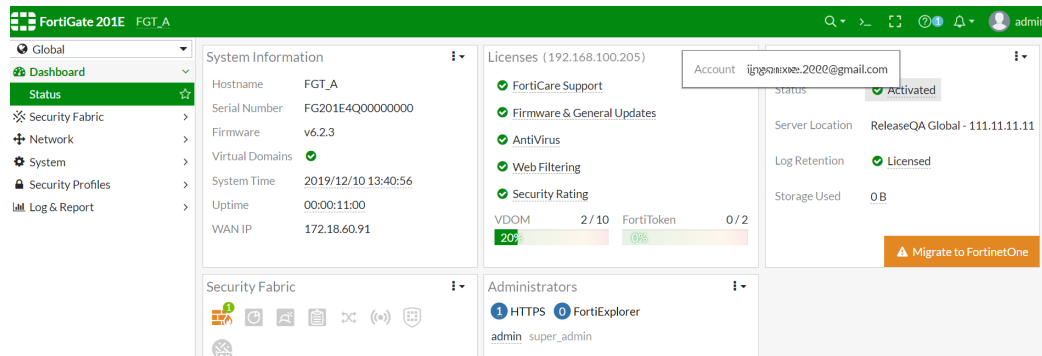


4. Click OK.
The FortiGate Cloud widget now shows the FortiCloud account.

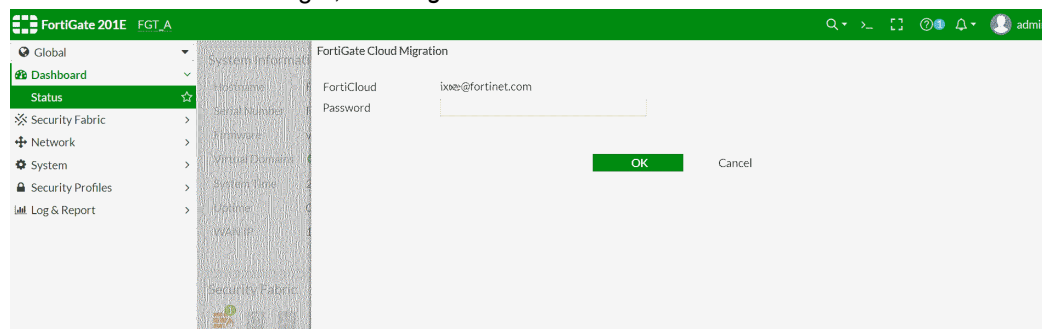


To migrate from the activated FortiGate Cloud account to the registered FortiCloud account:

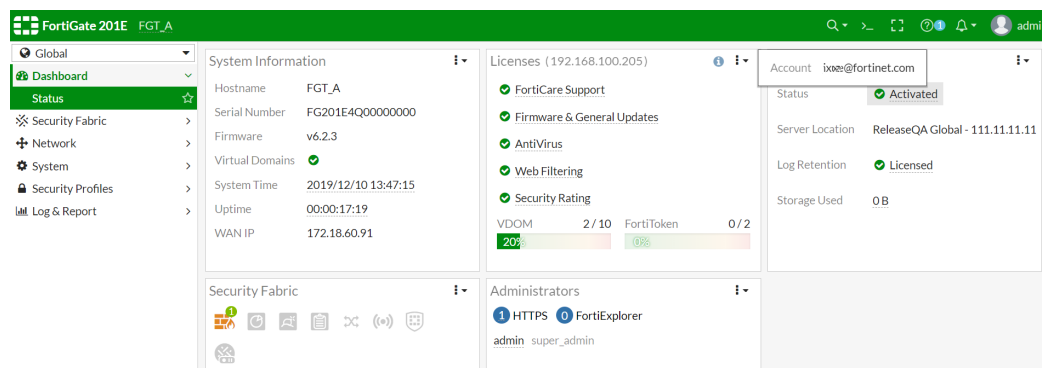
1. Go to *Dashboard > Status*.



2. In the FortiGate Cloud widget, click *Migrate to FortiCloud*.



3. Enter the password for the account that was used to register the FortiGate, then click *OK*.
The FortiGate Cloud widget now shows the FortiCloud account.



To activate FortiGate Cloud using an account that is not used for registration:

1. In the CLI, enter the following command:

```
execute fortiguard-log login <account_id> <password>
```

Where the <account_id> and <password> are the credentials for the account that you are using to activate FortiGate Cloud.

2. Check the account type with following command:

```
# diagnose fdsm contract-controller-update
Protocol=2.0|Response=202|Firmware=FAZ-4K-FW-2.50-
```

```
100|SerialNumber=FAMS000000000000|Persistent=false|ResponseItem=HomeServer:172.16.95.151:443*AlterServer:172.16.95.151:443*Contract:20200408*NextRequest:86400*UploadConfig:False*ManagementMode:Local*ManagementID:737941253*AccountType:multitenancy
```

```
Result=Success
```



A FortiCloud account that is not used for the support portal account cannot be used to register FortiGate. Attempting to activate FortiGate Cloud with this type of account will fail.

FortiGate Cloud

FortiGate Cloud is a hosted security management and log retention service for FortiGate devices. It provides centralized reporting, traffic analysis, configuration management, and log retention without the need for additional hardware or software.

FortiGate Cloud offers a wide range of features:

- **Simplified central management**

FortiGate Cloud provides a central GUI to manage individual or aggregated FortiGate and FortiWiFi devices. Adding a device to the FortiGate Cloud management subscription is straightforward. FortiGate Cloud has detailed traffic and application visibility across the whole network.

- **Hosted log retention with large default storage allocated**

Log retention is an integral part of any security and compliance program, but administering a separate storage system is onerous. FortiGate Cloud takes care of this automatically and stores the valuable log information in the cloud. Different types of logs can be stored, including Traffic, System Events, Web, Applications, and Security Events.

- **Monitoring and alerting in real time**

Network availability is critical to a good end-user experience. FortiGate Cloud enables you to monitor your FortiGate network in real time with different alerting mechanisms to pinpoint potential issues. Alerting mechanisms can be delivered via email.

- **Customized or pre-configured reporting and analysis tools**

Reporting and analysis are your eyes and ears into your network's health and security. Pre-configured reports are available, as well as custom reports that can be tailored to your specific reporting and compliance requirements. The reports can be emailed as PDFs, and can cover different time periods.

- **Maintain important configuration information uniformly**

The correct configuration of the devices within your network is essential for maintaining optimum performance and security posture. In addition, maintaining the correct firmware (operating system) level allows you to take advantage of the latest features.

- **Service security**

All communication (including log information) between the devices and the cloud is encrypted. Redundant data centers are always used to give the service high availability. Operational security measures have been put in place to make sure your data is secure — only you can view or retrieve it.

Registration and activation



Before you can activate a FortiGate Cloud account, you must first register your device.

FortiGate Cloud accounts can be registered manually through the FortiGate Cloud website, <https://www.forticloud.com>, or you can easily register and activate your account directly from your FortiGate.

To activate your FortiGate Cloud account:

1. On your device, go to *Dashboard > Status*.
2. In the *FortiGate Cloud* widget, click the *Not Activated > Activate* button in the *Status* field.
3. A pane will open asking you to register your FortiGate Cloud account. Click *Create Account*, enter your information, view and accept the terms and conditions, and then click *OK*.
4. A second dialogue window open, asking you to enter your information to confirm your account. This sends a confirmation email to your registered email. The dashboard widget then updates to show that confirmation is required.
5. Open your email, and follow the confirmation link it contains.
A FortiGate Cloud page will open, stating that your account has been confirmed. The *Activation Pending* message on the dashboard will change to state the type of account you have, and will provide a link to the FortiGate Cloud portal.

Enabling logging to FortiGate Cloud

To enable logging to FortiGate Cloud:

1. Go to *Security Fabric > Settings* or *Log & Report > Log Settings*.
2. Enable *Cloud Logging*.
3. Select an upload option: *Realtime*, *Every Minute*, or *Every 5 Minutes* (default).
4. Click *Apply*.

Logging into the FortiGate Cloud portal

Once logging has been configured and you have registered your account, you can log into the FortiGate Cloud portal and begin viewing your logging results. There are two methods to reach the FortiGate Cloud portal:

- If you have direct network access to the FortiGate:
 - a. Go to *Dashboard > Status*.
 - b. In the *FortiGate Cloud* widget, in the *Status* field, click *Activated > Launch Portal*, or, in the *Licenses* widget, click *FortiCare Support > Launch Portal*.
- If you do not have access to the FortiGate's interface, visit the FortiGate Cloud website (<https://www.forticloud.com>) and log in remotely, using your email and password. It will ask you to confirm the FortiGate Cloud account you are connecting to and then you will be granted access.

Cloud sandboxing

FortiGate Cloud can be used for automated sample tracking, or sandboxing, for files from a FortiGate. This allows suspicious files to be sent to be inspected without risking network security. If the file exhibits risky behavior, or is found to contain a virus, a new virus signature is created and added to the FortiGuard antivirus signature database.

To configure cloud sandboxing:

1. Go to *Security Fabric > Settings*.
2. Enable *Sandbox Inspection*.
3. Set the *FortiSandbox type* to *FortiSandbox Cloud*.



By default, the *FortiSandbox Cloud* option is not visible. See [Feature visibility on page 732](#) for instructions on making it visible.

4. Select the *FortiSandbox cloud region*.
5. Click *Apply*.

Sandboxing results are shown on the *Sandbox* tab in the FortiGate Cloud portal.

For more information about FortiGate Cloud, see the [FortiGate Cloud documentation](#).

Troubleshooting your installation

If your FortiGate does not function as desired after installation, try the following troubleshooting tips:

1. Check for equipment issues

Verify that all network equipment is powered on and operating as expected. Refer to the QuickStart Guide for information about connecting your FortiGate to the network.

2. Check the physical network connections

Check the cables used for all physical connections to ensure that they are fully connected and do not appear damaged, and make sure that each cable connects to the correct device and the correct Ethernet port on that device.

3. Verify that you can connect to the internal IP address of the FortiGate

Connect to the GUI from the FortiGate's internal interface by browsing to its IP address. From the PC, try to ping the internal interface IP address; for example, `ping 192.168.1.99`. If you cannot connect to the internal interface, verify the IP configuration of the PC. If you can ping the interface but can't connect to the GUI, check the settings for administrative access on that interface. Alternatively, use SSH to connect to the CLI, and then confirm that HTTPS has been enabled for Administrative Access on the interface.

4. Check the FortiGate interface configurations

Check the configuration of the FortiGate interface connected to the internal network (under *Network > Interfaces*) and check that *Addressing mode* is set to the correct mode.

5. Verify the security policy configuration

Go to *Policy & Objects > IPv4 Policy* and verify that the internal interface to Internet-facing interface security policy has been added and is located near the top of the policy list. Check the *Active Sessions* column to ensure that traffic has been processed (if this column does not appear, right-click on the table header and select *Active Sessions*). If

you are using NAT mode, check the configuration of the policy to make sure that *NAT* is enabled and that *Use Outgoing Interface Address* is selected.

6. Verify the static routing configuration

Go to *Network > Static Routes* and verify that the default route is correct. Go to *Monitor > Routing Monitor* and verify that the default route appears in the list as a static route. Along with the default route, you should see two routes shown as *Connected*, one for each connected FortiGate interface.

7. Verify that you can connect to the Internet-facing interface's IP address

Ping the IP address of the Internet-facing interface of your FortiGate. If you cannot connect to the interface, the FortiGate is not allowing sessions from the internal interface to Internet-facing interface. Verify that PING has been enabled for *Administrative Access* on the interface.

8. Verify that you can connect to the gateway provided by your ISP

Ping the default gateway IP address from a PC on the internal network. If you cannot reach the gateway, contact your ISP to verify that you are using the correct gateway.

9. Verify that you can communicate from the FortiGate to the Internet

Access the FortiGate CLI and use the command `execute ping 8.8.8.8`. You can also use the `execute traceroute 8.8.8.8` command to troubleshoot connectivity to the Internet.

10. Verify the DNS configurations of the FortiGate and the PCs

Check for DNS errors by pinging or using traceroute to connect to a domain name; for example: `ping www.fortinet.com`.

If the name cannot be resolved, the FortiGate or PC cannot connect to a DNS server and you should confirm that the DNS server IP addresses are present and correct.

11. Confirm that the FortiGate can connect to the FortiGuard network

Once the FortiGate is on your network, you should confirm that it can reach the FortiGuard network. First, check the *License Information* widget to make sure that the status of all FortiGuard services matches the services that you have purchased. Go to *System > FortiGuard*. Scroll down to *Filtering Services Availability* and select *Check Again*. After a minute, the GUI should indicate a successful connection. Verify that your FortiGate can resolve and reach FortiGuard at `service.fortiguard.net` by pinging the domain name. If you can reach this service, you can then verify the connection to FortiGuard servers by running the command `diagnose debug rating`. This displays a list of FortiGuard IP gateways you can connect to, as well as the following information:

- **Weight:** Based on the difference in time zone between the FortiGate and this server
- **RTT:** Return trip time
- **Flags:** D (IP returned from DNS), I (Contract server contacted), T (being timed), F (failed)
- **TZ:** Server time zone
- **Curr Lost:** Current number of consecutive lost packets
- **Total Lost:** Total number of lost packets

12. Consider changing the MAC address of your external interface

Some ISPs do not want the MAC address of the device connecting to their network cable to change. If you have added a FortiGate to your network, you may have to change the MAC address of the Internet-facing interface using the following CLI command:

```
config system interface
  edit <interface>
    set macaddr <xx:xx:xx:xx:xx:xx>
  end
end
```

13. Check the FortiGate bridge table (transparent mode)

When a FortiGate is in transparent mode, the unit acts like a bridge sending all incoming traffic out on the other interfaces. The bridge is between interfaces on the FortiGate unit. Each bridge listed is a link between interfaces. Where traffic is flowing between interfaces, you expect to find bridges listed. If you are having connectivity issues

and there are no bridges listed, that is a likely cause. Check for the MAC address of the interface or device in question. To list the existing bridge instances on the FortiGate, use the following CLI command:

```
diagnose netlink brctl name host root.b
show bridge control interface root.b host.
fdb: size=2048, used=25, num=25, depth=1
Bridge root.b host table
port no device devname mac addr ttl attributes
3 4 wan1 00:09:0f:cb:c2:77 88
3 4 wan1 00:26:2d:24:b7:d3 0
3 4 wan1 00:13:72:38:72:21 98
4 3 internal 00:1a:a0:2f:bc:c6 6
1 6 dmz 00:09:0f:dc:90:69 0 Local Static
3 4 wan1 c4:2c:03:0d:3a:38 81
3 4 wan1 00:09:0f:15:05:46 89
3 4 wan1 c4:2c:03:1d:1b:10 0
2 5 wan2 00:09:0f:dc:90:68 0 Local Static
```

14. Use FortiExplorer if you can't connect to the FortiGate over Ethernet

If you can't connect to the FortiGate GUI or CLI, you may be able to connect using FortiExplorer. Refer to the QuickStart Guide or see the section on FortiExplorer for more details.

15. Either reset the FortiGate to factory defaults or contact Fortinet Support for assistance

To reset the FortiGate to factory defaults, use the CLI command `execute factoryreset`. When prompted, type `y` to confirm the reset.

If you require further assistance, visit the [Fortinet Support](#) website.

Zero touch provisioning

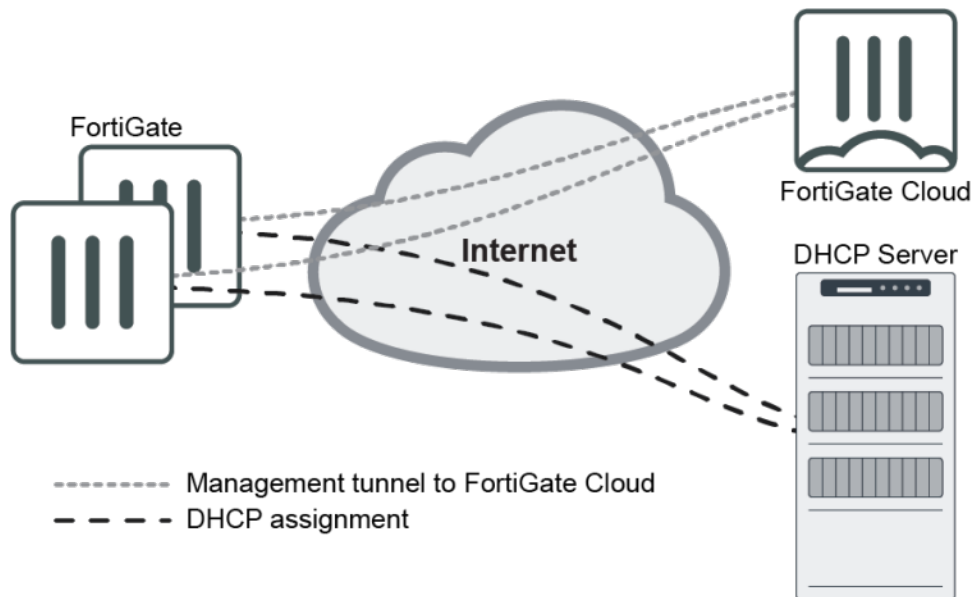
This section contains instructions for configuring zero touch provisioning:

- [Zero touch provisioning with FortiDeploy on page 53](#)
- [Zero touch provisioning with FortiManager on page 56](#)

Zero touch provisioning with FortiDeploy

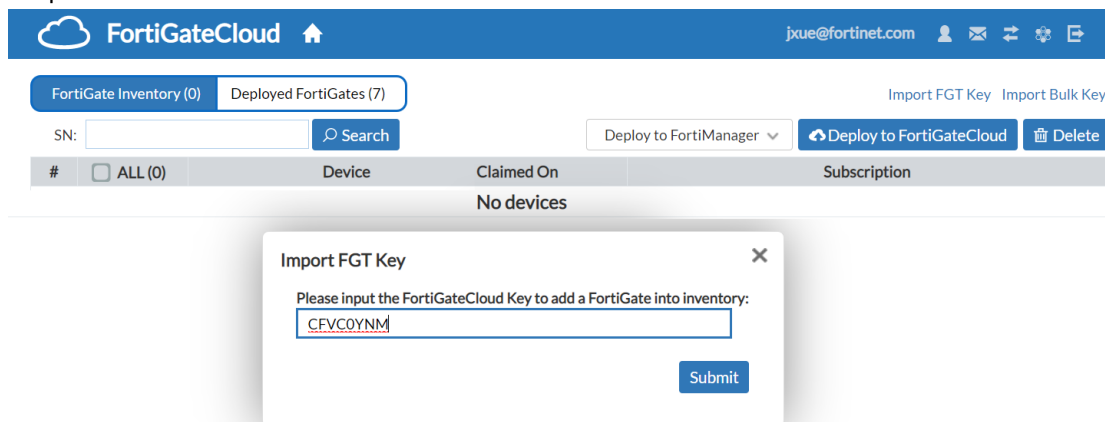
You can use this feature only when the FortiGate boots up from factory reset.

Topology

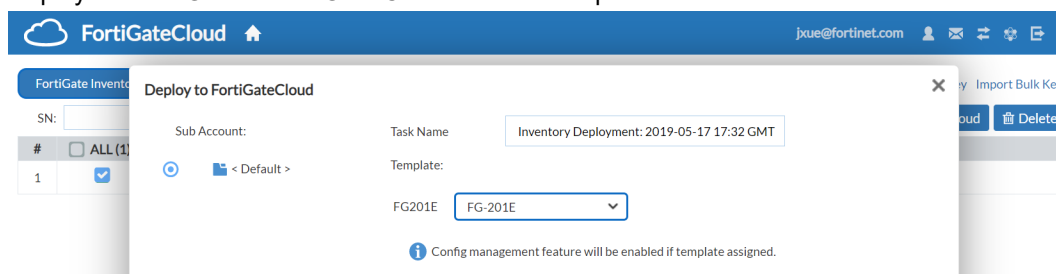


FortiGate zero touch provisioning workflow

1. Add the FortiGate Cloud product key to the FortiGate Cloud portal so that the FortiGate serial number appears in the portal.



2. Set up a configuration template with the basic configuration in the FortiGate Cloud portal.
3. Deploy the FortiGate to FortiGate Cloud with that template.



4. Ensure the FortiGate has an interface in default DHCP client mode and is connected to the ISP outlet.

5. Boot the FortiGate in factory reset. The FortiGate gets the DHCP lease so that it can access FortiGate Cloud in the Internet and join FortiGate Cloud.

```
Initializing firewall...
System is starting...
```

```
FortiGate-201E login: admin
Password:
Welcome !
FortiGate-201E #
```

```
FortiGate-201E # diagnose debug cli 7
Debug messages will be on for 30 minutes.
FortiGate-201E # 0: config system fortiguard
0: set service-account-id "jxue@fortinet.com"
0: end
0: config log fortiguard setting
0: set status enable
0: end
FortiGate-201E # diagnose test application forticldd 1
System=FGT Platform=FG201E
Management vdom: root, id=0, ha=master.
acct_id=jxue@fortinet.com
acct_st=OK
FortiGuard log: status=enabled, full=overwrite, ssl_opt=1, source-ip=0.0.0.0
Centra Management: type=FGD, flags=000000bf.
active-tasks=0
```

The FortiGate Cloud server checks that the FortiGate key is valid and then deploys the FortiGate to FortiGate Cloud.

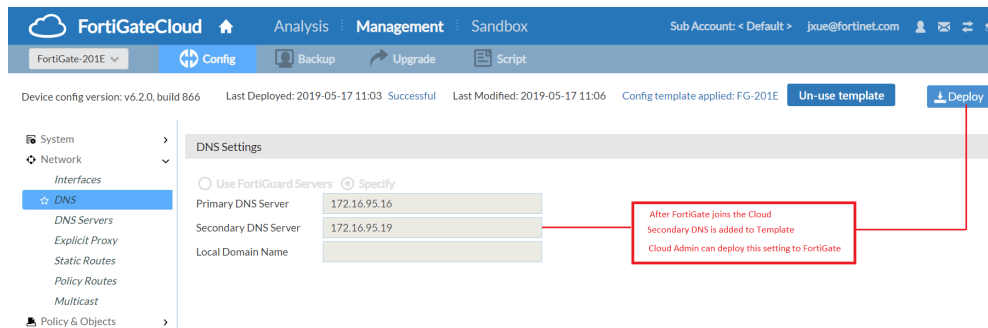
To prevent spoofing, FortiGate Cloud invalidates that key after a successful join.

6. Complete zero touch provisioning by obtaining configuration from platform template in the Cloud.

```
0:      set admintimeout 50
0: end
0: config system interface
0:      edit "wan1"
0:          set allowaccess ping ssh fgfm
0:      next
0:      edit "port1"
0:          set allowaccess ping
0:          set ip 1.1.1.1 255.255.255.0
0:      next
0:      edit "port2"
0:          set allowaccess ping
0:          set ip 2.2.2.2 255.255.255.0
0:      next
0: end
```

7. The FortiGate Cloud admin can change the template for different configuration requirements and then deploy the updated template to the FortiGate.

For example, you can add a secondary DNS to the template and deploy it to FortiGate.



Zero touch provisioning with FortiManager

You can use this feature only when the FortiGate boots up from factory reset. This feature is for FortiGate devices that cannot access the Internet.

A DHCP server includes option 240 and 241 which records FortiManager IP and domain name. FortiGate has an interface with the default DHCP client mode that is connected to the DHCP server in the intranet.

The FortiManager admin can authorize the FortiGate the specific ADOMs and install specific configurations on the FortiGate.

In the whole operation, you do not need to do any manual configuration on the FortiGate except connect to the DHCP server. This is called zero touch deployment.

To prevent spoofing, if a different FortiManager IP comes from the DHCP server later, FortiGate does not change the central management configuration.

Example of configuring DHCP server with option 240

```
config system dhcp server
  edit 2
    set dns-service default
    set default-gateway 172.16.200.254
    set netmask 255.255.255.0
    set interface "wan1"
    config ip-range
      edit 2
        set start-ip 172.16.200.201
        set end-ip 172.16.200.209
      next
    end
    set timezone-option default
    config options
      edit 1
        set code 240
        set type ip
        set ip "172.18.60.115"
      next
    end
  next
end
```

FortiGate zero touch provisioning workflow

1. Boot the FortiGate in factory reset.

```
G201E4Q17901047 # diagnose fdsm fmg-auto-discovery-status
dhcp: fmg-ip=0.0.0.0, fmg-domain-name='', config-touched=0
```

config-touched=0 means no configuration change from the default.

2. When FortiGate boots in factory reset, it gets the DHCP lease including IP, gateway, DNS, and the FortiManager IP/URL. Central management is automatically configured by using FortiManager IP in option 240.

```
FG201E4Q17901047 # show system central-management
config system central-management
    set type fortimanager
    set fmg "172.18.60.115"
end
```

3. If FortiGate changes from factory reset, you can see it in central management in config-touched=1.

```
FG201E4Q17901047 # diagnose fdsm fmg-auto-discovery-status
dhcp: fmg-ip=172.18.60.115, fmg-domain-name='', config-touched=1 (/bin/dhcpd)
```

Example of a spoofing DHCP server with a fake FortiManager IP

```
config options
    edit 1
        set code 240
        set type ip
        set ip "172.18.60.117"
    end
```

After FortiGate reboots and gets DHCP renew, central management will not use the fake FortiManager IP because config-touched=1 shows that the FortiGate is not in factory reset.

```
FG201E4Q17901047 # diagnose fdsm fmg-auto-discovery-status
dhcp: fmg-ip=0.0.0.0, fmg-domain-name='', config-touched=1 (/bin/dhcpd)
```

```
FG201E4Q17901047 # show system central-management
config system central-management
    set type fortimanager
    set fmg "172.18.60.115"
end
```

Dashboard

FortiOS dashboards can have a Network Operations Center (NOC) or responsive layout.

- On a responsive dashboard, the number of columns is determined by the size of the screen. Widgets can only be resized horizontally, but the dashboard will fit on all screen sizes.
- On a NOC dashboard, the number of columns is explicitly set. Widgets can be resized both vertically and horizontally, but the dashboard will look best on the screen size that it is configured for.

Multiple dashboards of both types can be created, for both individual VDOMs and globally. Widgets are interactive; clicking or hovering over most widgets shows additional information or links to relevant pages. Widgets can be reorganized by clicking and dragging them around the screen.

Four dashboards are available by default: *Status*, *Top Usage LAN/DMZ*, *Security*, and *System Events*.

The *Status* dashboard includes the following widgets by default:

Widget	Description
System Information	The System Information widget lists information relevant to the FortiGate system, including hostname, serial number, and firmware. Clicking in the widget provides links to configure system settings and update the device firmware.
Licenses	The Licenses widget lists the status of various licenses, such as FortiCare Support and IPS. The number of used and available FortiTokens is also shown. Clicking in the widget provides a link to the FortiGuard settings page.
Virtual Machine	The VM widget (shown by default in the dashboard of a FortiOS VM device) includes: <ul style="list-style-type: none">• License status and type• vCPU allocation and usage• RAM allocation and usage• VMX license information (if the VM supports VMX) Clicking on an item in the widget provides a link to the <i>FortiGate VM License</i> page, where license files can be uploaded.
FortiGate Cloud	This widget displays the FortiGate Cloud and FortiSandbox Cloud status. See FortiGate Cloud on page 93 for more information.
Security Fabric	The Security Fabric widget displays a visual summary of the devices in the Fortinet Security Fabric. Clicking on a product icon provides a link to a page relevancy to that product. For example, clicking the FortiAnalyzer shows a link to log settings. See Security Fabric status on page 91 for more information.
Security Rating	The Security Rating widget shows the security rating for your Security Fabric. It can show the current rating percentile, or historical security rating score or percentile charts. See Security Rating on page 91 for more information.

Widget	Description
Administrators	This widget allows you to see logged in administrators, connected administrators, and the protocols used by each. Clicking in the widget provides links to view active administrator sessions, and to open the FortiExplorer page on the App Store.
CPU	This widget shows real-time CPU usage over the selected time frame. Hovering over any point on the graph displays the percentage of CPU power used at that specific time. It can be expanded to occupy the entire dashboard.
Memory	This widget shows real-time memory usage over the selected time frame. Hovering over any point on the graph displays the percentage of the memory used at that specific time. It can be expanded to occupy the entire dashboard.
Sessions	This widget shows the current number of sessions over the selected time frame. Hovering over any point on the graph displays the number of sessions at that specific time. It can be expanded to occupy the entire dashboard.

The *Top Usage LAN/DMZ* dashboard includes the following widgets by default:

Widget	Description
Top Sources by Bytes	This widget lists the top sources by the number of bytes used.
Top Destinations by Sessions	This widget lists the top destinations by the number of sessions.
Top Applications by Bytes	This widget lists the top applications by the number of bytes used.
Top Web Site by Sessions	This widget lists the top websites by the number of sessions.

The *Security* dashboard includes the following widgets by default:

Widget	Description
Top Compromised Hosts by Verdict	This widget lists the compromised hosts by verdict. A FortiAnalyzer is required. It can be expanded to occupy the entire dashboard.
Top Threats by Threat Level	This widget lists the top threats by threat level from FortiView. It can be expanded to occupy the entire dashboard.
FortiClient Detected Vulnerabilities	This widget shows the number of vulnerabilities detected by FortiClient. FortiClient must be enabled. Clicking in the widget provides a link to view the information in FortiView.
Host Scan Summary	This widget lists the total number of hosts. Clicking in the widget provides links to view vulnerable device in FortiView, FortiClient monitor, and the device inventory.

Widget	Description
Top Vulnerable Endpoint Devices by Detected Vulnerabilities	This widget lists the top vulnerable endpoints by the detected vulnerabilities, from FortiView. It can be expanded to occupy the entire dashboard.

The *System Events* dashboard includes the following widgets by default:

Widget	Description
Top System Events by Events	This widget lists the top system events, sorted by the number of events. It can be expanded to occupy the entire dashboard. Double click on an event to view the specific event log.
Top System Events by Level	This widget lists the top system events, sorted by the events' levels. It can be expanded to occupy the entire dashboard. Double click on an event to view the specific event log.

The following optional widgets can also be added to a dashboard:

Widget	Description
FortiView Top N	This widget shows the top items from the selected FortiView category. The widget's title, time period, visualization (table or bubble chart), and what the data is sorted by can all be customized.
Botnet Activity	This widget shows information about botnet activity. Clicking in the widget provides links to check botnet activity, view FortiGuard package information, view IPS logs, and view DNS query logs.
HA Status	This widget shows the HA mode of the device. Clicking in the widget provides a link to HA settings.
Disk Usage	This widget shows real-time disk usage over the selected time frame. Hovering over any point on the graph displays the percentage of the disk used at that specific time. It can be expanded to occupy the entire dashboard.
Log Rate	This widget shows the real-time log rate over the selected time frame. Hovering over any point on the graph displays the log rate at that specific time. Clicking in the widget provides a link to log settings. It can be expanded to occupy the entire dashboard.
Session Rate	This widget shows the real-time session rate over the selected time frame. Hovering over any point on the graph displays the session rate at that specific time. It can be expanded to occupy the entire dashboard.
Fabric Device	This widget shows statistics and system information about the selected fabric device. See Fabric Device on page 92 for more information.
Advanced Threat Protection Statistics	This widget shows threat protection statistics, including the number of scanned files and how many scanned files there are for each threat level.

Widget	Description
Interface Bandwidth	<p>This widget shows the real-time incoming and outgoing traffic bandwidth of the selected interface over the selected time frame. Hovering over any point on the graph displays the bandwidth at that specific time.</p> <p>Clicking and dragging over a portion of the graph provides a link to view the data from the highlighted time frame in FortiView.</p> <p>A maximum of 25 interfaces can be monitored at one time on a device.</p>

Dashboard CLI

Dashboards and widgets can be managed using the CLI. The options available when creating a widget will vary depending on the widget type.

To create a dashboard:

```
config system admin
  edit <admin name>
    config gui-dashboard
      edit <dashboard number>
        set name <name>
        set vdom <vdom>
        set layout-type {responsive | fixed}
        set permanent {enable | disable}
      next
    end
  next
end
```

To add a widget to a dashboard:

```
config system admin
  edit <admin name>
    config gui-dashboard
      edit <dashboard number>
        config widget
          edit <widget number>
            set type <widget type>
            set x-pos <0 - 1000>
            set y-pos <0 - 1000>
            set width <1 - 50>
            set height <1 - 50>
            ...
          next
        end
      next
    end
  next
end
```

The widget type can be one of the following:

CLI type	GUI name
sysinfo	System Information
licinfo	License Information
vminfo	Virtual machine information
forticloud	FortiGate Cloud Licenses
cpu-usage	CPU Usage
memory-usage	Memory Usage
disk-usage	Disk Usage
log-rate	Session Rate
sessions	Sessions
session-rate	Session Rate
tr-history	Traffic History
analytics	FortiGuard Analytics
usb-modem	USB Modem
admins	Administrators
security-fabric	Security Fabric
security-fabric-ranking	Security Fabric Ranking
ha-status	HA Status
vulnerability-summary	Vulnerability Summary
host-scan-summary	Host Scan Summary
fortiview	FortiView
botnet-activity	Botnet Activity
fabric-device	Fabric Device

Configuration backups

Once you successfully configure the FortiGate, it is extremely important that you backup the configuration. In some cases, you may need to reset the FortiGate to factory defaults or perform a TFTP upload of the firmware, which will erase the existing configuration. In these instances, the configuration on the device will have to be recreated, unless a backup can be used to restore it. You should also backup the local certificates, as the unique SSL inspection CA and server certificates that are generated by your FortiGate by default are not saved in a system backup.

We also recommend that you backup the configuration after *any* changes are made, to ensure you have the most current configuration available. Also, backup the configuration before any upgrades of the FortiGate's firmware. Should anything happen to the configuration during the upgrade, you can easily restore the saved configuration.

Always backup the configuration and store it on the management computer or off-site. You have the option to save the configuration file to various locations including the local PC, USB key, FTP, and TFTP server. The last two are configurable through the CLI only.

If you have VDOMs, you can back up the configuration of the entire FortiGate or only a specific VDOM. Note that if you are using FortiManager or FortiGate Cloud, full backups are performed and the option to backup individual VDOMs will not appear.



You can also backup and restore your configuration using Secure File Copy (SCP). See [How to download/upload a FortiGate configuration file using secure file copy \(SCP\)](#).

You enable SCP support using the following command:

```
config system global
    set admin-scp enable
end
```

For more information about this command and about SCP support, see [config system global](#).

Backing up the configuration

To backup the configuration using the GUI:

1. Click on the user name in the upper right-hand corner of the screen and select *Configuration > Backup*.
2. Direct the backup to your *Local PC* or to a *USB Disk*.
The *USB Disk* option will not be available if no USB drive is inserted in the USB port. You can also backup to the FortiManager using the CLI.
3. If VDOMs are enabled, indicate whether the scope of the backup is the entire FortiGate configuration (*Global*) or only a specific VDOM configuration (*VDOM*).
If backing up a VDOM configuration, select the VDOM name from the list.
4. Enable *Encryption*. Encryption must be enabled on the backup file to back up VPN certificates.
5. Enter a password, and enter it again to confirm it. This password will be required to restore the configuration.
6. Click *OK*.
7. When prompted, select a location on the PC or USB disk to save the configuration file. The configuration file will have a .conf extension.

To backup the configuration using the CLI:

Use one of the following commands:

```
execute backup config management-station <comment>
```

or:

```
execute backup config usb <backup_filename> [<backup_password>]
```

or for FTP, note that port number, username are optional depending on the FTP site:

```
execute backup config ftp <backup_filename> <ftp_server> [<port>] [<user_name>]
[<password>]
```

or for TFTP:

```
execute backup config tftp <backup_filename> <tftp_servers> <password>
```

Use the same commands to backup a VDOM configuration by first entering the commands:

```
config vdom
```

```
edit <vdom_name>
```

Restoring a configuration

To restore the FortiGate configuration using the GUI:

1. Click on the user name in the upper right-hand corner of the screen and select *Configuration > Restore*.
2. Identify the source of the configuration file to be restored: your *Local PC* or a *USB Disk*.
The *USB Disk* option will not be available if no USB drive is inserted in the USB port. You can restore from the FortiManager using the CLI.
3. Click Upload, locate the configuration file, and click *Open*.
4. Enter the password if required.
5. Click *OK*.

To restore the FortiGate configuration using the CLI:

```
execute restore config management-station normal 0
```

or:

```
execute restore config usb <filename> [<password>]
```

or for FTP, note that port number, username are optional depending on the FTP site:

```
execute restore config ftp <backup_filename> <ftp_server> [<port>] [<user_name>]  
[<password>]
```

or for TFTP:

```
execute restore config tftp <backup_filename> <tftp_server> <password>
```

The FortiGate will load the configuration file and restart. Once the restart has completed, verify that the configuration has been restored.

Troubleshooting

When restoring a configuration, errors may occur, but the solutions are usually straightforward.

Error message	Reason and Solution
Configuration file error	<p>This error occurs when attempting to upload a configuration file that is incompatible with the device. This may be due to the configuration file being for a different model or being saved from a different version of firmware.</p> <p>Solution: Upload a configuration file that is for the correct model of FortiGate device and the correct version of the firmware.</p>
Invalid password	<p>When the configuration file is saved, it can be protected by a password. The password entered during the upload process is not matching the one associated with the configuration file.</p> <p>Solution: Use the correct password if the file is password protected.</p>

Configuration revision

You can manage multiple versions of configuration files on models that have a 512MB flash memory and higher. Revision control requires either a configured central management server or the local hard drive, if your FortiGate has this feature. Typically, configuration backup to local drive is not available on lower-end models.

The central management server can either be a FortiManager unit or FortiGate Cloud.

If central management is not configured on your FortiGate unit, a message appears instructing you to either

- Enable central management, or
- Obtain a valid license.

When revision control is enabled on your FortiGate unit, and configuration backups have been made, a list of saved revisions of those backed-up configurations appears.

Configuration revisions are viewed by clicking on the user name in the upper right-hand corner of the screen and selecting *Configuration > Revisions*.

Backup and restore the local certificates

This procedure exports a server (local) certificate and private key together as a password protected PKCS12 file. The export file is created through a customer-supplied TFTP server. Ensure that your TFTP server is running and accessible to the FortiGate before you enter the command.

To back up the local certificates:

Connect to the CLI and use the following command:

```
execute vpn certificate local export tftp <cert_name> <filename> <tftp_ip>
```

where:

- <cert_name> is the name of the server certificate.
- <filename> is a name for the output file.
- <tftp_ip> is the IP address assigned to the TFTP server host interface.

To restore the local certificates using the GUI:

1. Move the output file from the TFTP server location to the management computer.
2. Go to *System > Certificates* and click *Import > Local*.
3. Select the certificate type, then click *Upload* in the *Certificate file* field.
4. On the management computer, browse to the file location, select it, and click *Open*.
5. If the *Type* is *Certificate*, upload the *Key file* as well.
6. If required, enter the *Password* that is required to upload the file or files.
7. Click *OK*.

To restore the local certificates using the CLI:

Connect to the CLI and use the following command:

```
execute vpn certificate local import tftp <filename> <tftp_ip>
```

Restore factory defaults

There may be a need to reset the FortiGate to its original defaults; for example, to begin with a fresh configuration. There are two options when restoring factory defaults. The first resets the entire device to the original out-of-the-box configuration.

You can reset the device with the following CLI command:

```
execute factoryreset
```

When prompted, type `y` to confirm the reset.

Alternatively, in the CLI you can reset the factory defaults but retain the interface and VDOM configuration with the following command:

```
execute factoryreset2
```


Fortinet Security Fabric

The Fortinet Security Fabric provides an intelligent architecture that interconnects discrete security solutions into an integrated whole to detect, monitor, block, and remediate attacks across the entire attack surface. It delivers broad protection and visibility into every network segment and device, be they hardware, virtual, or cloud based.

- The physical topology view shows all connected devices, including access layer devices. The logical topology view shows information about the interfaces that each device is connected to.
- Security rating checks analyze the Security Fabric deployment to identify potential vulnerabilities and highlight best practices to improve the network configuration, deploy new hardware and software, and increase visibility and control of the network.
- Fabric connectors provide integration with multiple SDN, cloud, and partner technology platforms to automate the process of managing dynamic security updates without manual intervention.
- Automation pairs an event trigger with one or more actions to monitor the network and take the designated actions automatically when the Security Fabric detects a threat.

Security Fabric settings and usage

This section contains information about the Fortinet Security Fabric settings and usage:

- [Components on page 68](#)
- [Configuring the root FortiGate and downstream FortiGates on page 70](#)
- [Configuring FortiAnalyzer on page 75](#)
- [Configuring other Security Fabric devices on page 76](#)
- [Using the Security Fabric on page 90](#)
- [Deploying the Security Fabric on page 103](#)
- [Security Fabric over IPsec VPN on page 111](#)
- [Leveraging LLDP to simplify Security Fabric negotiation on page 117](#)

System requirements

To set up the Security Fabric, the devices that you want to include must meet the Product Integration and Support requirements in the [FortiOS Release Notes](#).

Some features of the Security Fabric are only available in certain firmware versions and models. Not all FortiGate models can run the FortiGuard Security Rating Service if they are the root FortiGate in a Security Fabric. For more information, see the Special Notices in the [FortiOS Release Notes](#).

Prerequisites

- If devices are not already installed in your network, complete basic installation and configuration tasks by following the instructions in the device documentation.

- FortiGate devices must either have VDOMs disabled or be running in split-task VDOM mode in order to be added to the Security Fabric. See [Virtual Domains on page 650](#).
- FortiGate devices must be operating in NAT mode.

Components

The Fortinet Security Fabric consists of different components that work together to secure your network.

The following devices are required to create a Security Fabric:

Device	Description
FortiGate	<p>FortiGate devices are the core of the Security Fabric and can have one of the following roles:</p> <ul style="list-style-type: none"> • Root: The root FortiGate is the main component in the Security Fabric. It is typically located on the edge of the network and connects the internal devices and networks to the Internet through your ISP. From the root FortiGate, you can see information about the entire Security Fabric on the Physical and Logical Topology pages in the GUI. • Downstream: After a root FortiGate is installed, all other FortiGate devices in the Security Fabric act as Internal Segmentation Firewalls (ISFWs), located at strategic points in your internal network, rather than on the network edge. This allows extra security measures to be taken around key network components, such as servers that contain valuable intellectual property. ISFW FortiGate devices create network visibility by sending traffic and information about the devices that are connected to them to the root FortiGate. <p>See Configuring the root FortiGate and downstream FortiGates on page 70 for more information about adding FortiGate devices in the Security Fabric.</p> <p>FortiGate documentation: https://docs.fortinet.com/product/fortigate</p>
FortiAnalyzer	<p>FortiAnalyzer gives you increased visibility into your network, centralized monitoring, and awareness of threats, events, and network activity by collecting and correlating logs from all Security Fabric devices. This gives you a deeper and more comprehensive view across the entire Security Fabric.</p> <p>See Configuring FortiAnalyzer on page 75 for more information about adding FortiAnalyzer devices in the Security Fabric.</p> <p>FortiAnalyzer documentation: https://docs.fortinet.com/product/fortianalyzer</p>

The following devices are recommended:

Device	Description
FortiADC	<p>FortiADC devices optimize the availability, user experience, and scalability of enterprise application delivery. They enable fast, secure, and intelligent acceleration and distribution of even the most demanding enterprise applications.</p> <p>See Additional devices on page 88 for more information about adding FortiADC devices in the Security Fabric.</p> <p>FortiADC documentation: https://docs.fortinet.com/product/fortiadc</p>

Device	Description
FortiAP	<p>Add FortiAP devices to extend the Security Fabric to your wireless devices. Devices connected to a FortiAP appear in the Physical and Logical Topology pages in the Security Fabric menu.</p> <p>See FortiAP and FortiSwitch on page 88 for more information about adding FortiAP devices in the Security Fabric.</p> <p>FortiAP documentation: https://docs.fortinet.com/product/fortiap</p>
FortiClient	<p>FortiClient adds endpoint control to devices that are located in the Security Fabric, allowing only traffic from compliant devices to flow through the FortiGate. FortiClient compliance profiles are applied by the first FortiGate that a device's traffic flows through. Device registration and on-net status information for a device that is running FortiClient appears only on the FortiGate that applies the FortiClient profile to that device.</p> <p>FortiClient documentation: https://docs.fortinet.com/product/forticlient</p>
FortiClient EMS	<p>FortiClient EMS is used in the Security Fabric to provide visibility across your network, securely share information, and assign security profiles to endpoints.</p> <p>See FortiClient EMS on page 85 for more information about adding FortiClient EMS devices in the Security Fabric.</p> <p>FortiClient EMS documentation: https://docs.fortinet.com/product/forticlient</p>
FortiDDoS	<p>FortiDDoS is a Network Behavior Anomaly (NBA) prevention system that detects and blocks attacks that intend to disrupt network service by overutilizing server resources.</p> <p>See Additional devices on page 88 for more information about adding FortiDDoS devices in the Security Fabric.</p> <p>FortiDDoS documentation: https://docs.fortinet.com/product/fortiddos</p>
FortiMail	<p>FortiMail antispam processing helps offload from other devices in the Security Fabric that would typically carry out this process.</p> <p>See Additional devices on page 88 for more information about adding FortiMail devices in the Security Fabric.</p> <p>FortiMail documentation: https://docs.fortinet.com/product/fortimail</p>
FortiManager	<p>Add FortiManager to simplify the network management of devices in the Security Fabric by centralizing management access in a single device. This allows you to easily control the deployment of security policies, FortiGuard content security updates, firmware revisions, and individual configurations for devices in the Security Fabric.</p> <p>See FortiManager on page 81 for more information about adding FortiManager devices in the Security Fabric.</p> <p>FortiManager documentation: https://docs.fortinet.com/product/fortimanager</p>
FortiSandbox	<p>Add FortiSandbox to your Security Fabric to improve security with sandbox inspection. Sandbox integration allows FortiGate devices in the Security Fabric to automatically receive signature updates from FortiSandbox and add the originating URL of any malicious file to a blocked URL list.</p> <p>See FortiSandbox on page 83 for more information about adding FortiSandbox devices in the Security Fabric.</p> <p>FortiSandbox documentation: https://docs.fortinet.com/product/fortisandbox</p>

Device	Description
FortiSwitch	<p>A FortiSwitch can be added to the Security Fabric when it is managed by a FortiGate that is in the Security Fabric with the FortiLink protocol, and connected to an interface with <i>Security Fabric Connection</i> enabled. FortiSwitch ports to become logical extensions of the FortiGate. Devices connected to the FortiSwitch appear in the Physical and Logical Topology pages in the Security Fabric menu, and security features, such as FortiClient compliance profiles, are applied to them.</p> <p>See FortiAP and FortiSwitch on page 88 for more information about adding FortiSwitch devices in the Security Fabric.</p> <p>FortiSwitch documentation: https://docs.fortinet.com/product/fortiswitch</p>
FortiWeb	<p>Add FortiWeb to defend the application attack surface from attacks that target application exploits. You can also configure FortiWeb to apply web application firewall features, virus scanning, and web filtering to HTTP traffic to help offload from other devices in the Security Fabric that would typically carry out these processes.</p> <p>See Additional devices on page 88 for more information about adding FortiWeb devices in the Security Fabric.</p> <p>FortiWeb documentation: https://docs.fortinet.com/product/fortiweb</p>
FortiWLC	<p>FortiWLC delivers seamless mobility and superior reliability with optimized client distribution and channel utilization. Both single and multi channel deployment options are supported, maximizing efficiency to make the most of available wireless spectrum.</p> <p>See Additional devices on page 88 for more information about adding FortiWLC devices in the Security Fabric.</p> <p>FortiWLC documentation: https://docs.fortinet.com/product/wireless-controller</p>

The following devices are optional:

Device	Description
Other Fortinet products	<p>Many other Fortinet products can be added to the Security Fabric, including FortiAuthenticator, FortiToken, FortiCache, and FortiSIEM.</p> <p>Documentation: https://docs.fortinet.com/</p>
Third-party products	<p>Third-party products that belong to the Fortinet Fabric-Ready Partner Program can be added to the Security Fabric.</p>

Configuring the root FortiGate and downstream FortiGates

The following procedures include configuration steps for a typical Security Fabric implementation, where the edge FortiGate is the root FortiGate, and the downstream FortiGate devices are all devices that are downstream from the root FortiGate.

Prerequisites

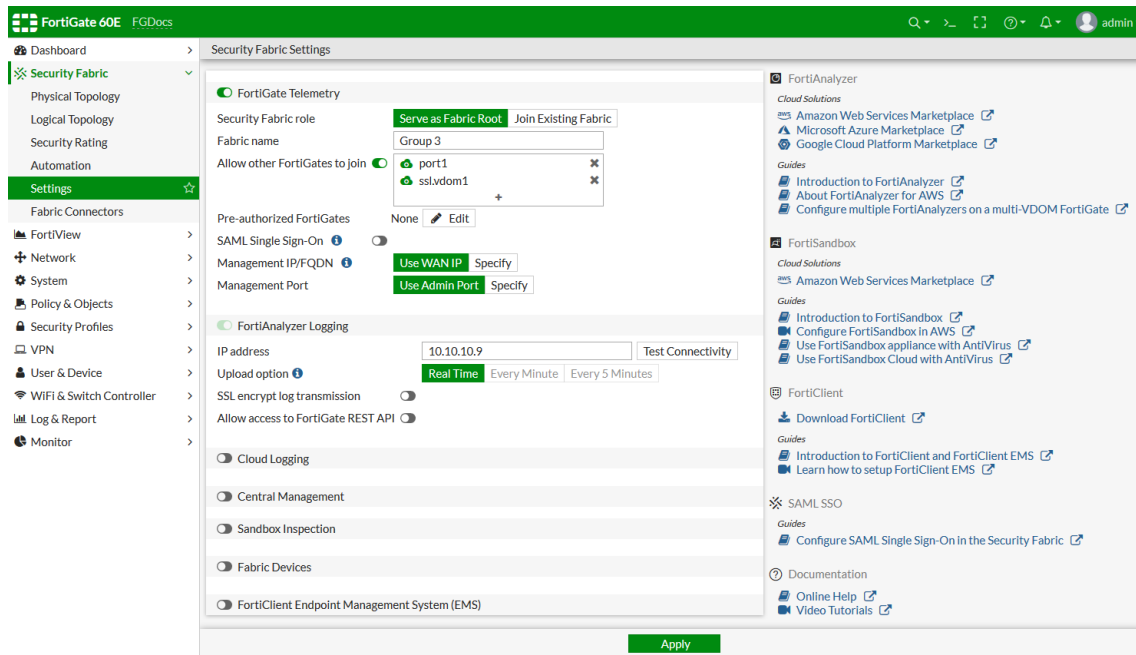
- FortiGate devices must either have VDOMs disabled or be running in split-task VDOM mode in order to be added to the Security Fabric. See [Virtual Domains on page 650](#).
- FortiGate devices must be operating in NAT mode.

Configure the root FortiGate

The edge FortiGate is typically configured as the root FortiGate, as this allows you to view the full topology of the Security Fabric from the top down.

To configure the root FortiGate:

1. Connect to the root FortiGate and go to *Security Fabric > Settings*.
2. Enable *FortiGate Telemetry*.
FortiAnalyzer Logging is automatically enabled.



3. Enter the *Fabric name*.
4. Enable *Allow other FortiGates to join*, and select interfaces.
5. In the *FortiAnalyzer Logging* section, in the *IP address* field, enter the IP address of the FortiAnalyzer. If you select *Test Connectivity* and this is the first time that you are connecting the FortiGate to the FortiAnalyzer, you will receive a warning message because the FortiGate has not yet been authorized on the FortiAnalyzer. You can configure this authorization when you configure the FortiAnalyzer. See [Configuring FortiAnalyzer on page 75](#).
6. If you need log transmissions to be encrypted, enable *SSL encrypt log transmission*.
7. If required, enable *Allow access to FortiGate REST API* and, optionally, *Trust FortiAnalyzer by serial number*. The REST API accesses the FortiGate topology and shares data and results. The FortiGate will verify the FortiAnalyzer by retrieving its serial number and checking it against the FortiAnalyzer certificate. When verified, the FortiAnalyzer serial number is stored in the FortiGate configuration. When authorizing the FortiGate on the FortiAnalyzer, the FortiGate admin credentials do not need to be entered.
8. Click *Apply*.

Add downstream devices

Downstream FortiGate devices can be securely added to the Security Fabric without sharing the password of the root FortiGate. Downstream device serial numbers can be authorized from the root FortiGate, or allowed to join by request.

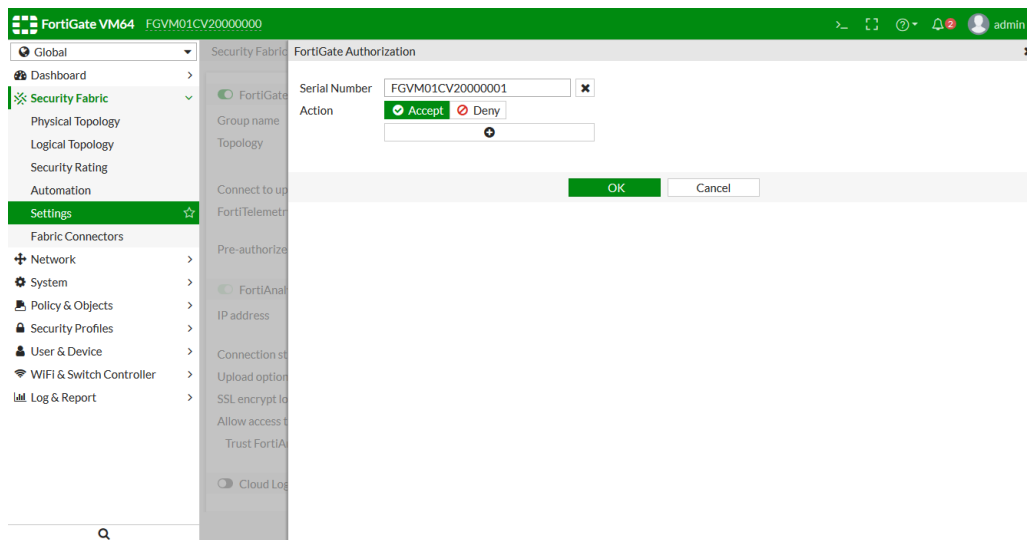
New authorization requests include the device serial number, IP address, and HA members. HA members can include up to four serial numbers and is used to ensure that, in the event of a fail over, the secondary FortiGate is still authorized.

Pre-authorizing the downstream FortiGate

When a downstream Fortinet device's serial number is added to the trusted list on the root FortiGate, the device can join the Security Fabric as soon as it connects. After the new device is authorized, connected FortiAP and FortiSwitch devices are automatically included in the topology, where they can be authorized with one click.

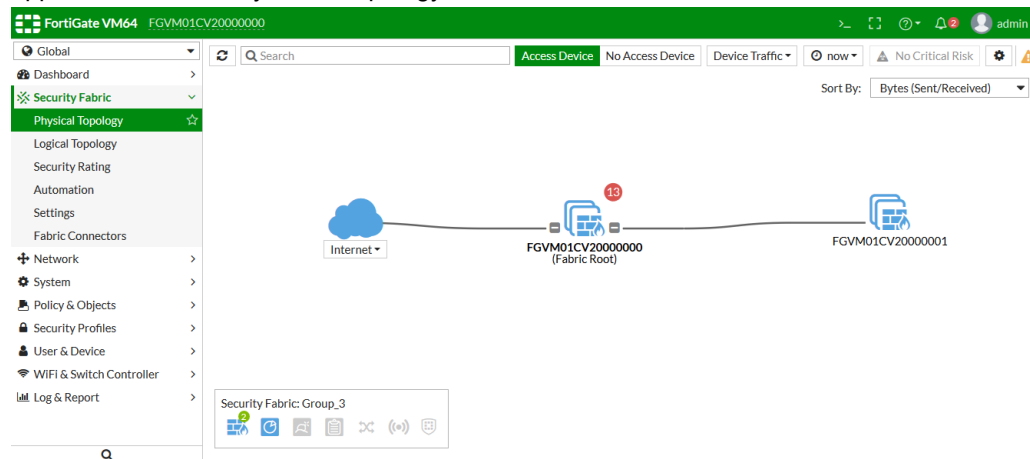
To pre-authorize a FortiGate:

1. On the root FortiGate, go to *Security Fabric > Settings*.
2. Ensure that the interface that connects to the downstream FortiGate has *Security Fabric Connection* enabled.
3. In the *Pre-authorized FortiGates*, select *Edit*. Add a new FortiGate to the list using the downstream device's serial number.



4. On the downstream FortiGate, go to *Security Fabric > Settings*.
5. Enable *FortiGate Telemetry*.
6. Set *Security Fabric role* to *Join Existing Fabric*.
7. Enter the IP address of the upstream or root FortiGate in the *Upstream FortiGate IP* field.
8. Click *Apply*.
9. On the root FortiGate, go to *Security Fabric > Settings* and verify that the downstream FortiGate that you added

appears in the Security Fabric topology.



Using LLDP

You can automatically prompt downstream FortiGate devices to join the Security Fabric using Link Layer Discovery Protocol (LLDP) and interface role assignments.

1. On the root FortiGate, assign the LAN role to all interfaces that may connect to downstream FortiGate devices. When the LAN role is assigned to an interface, LLDP transmission is enabled by default.
2. When a downstream FortiGate is installed, assign the WAN role to the interface that connects to the upstream FortiGate.
When the WAN role is assigned, LLDP reception is enabled by default. The newly installed FortiGate uses LLDP to discover the upstream FortiGate, and the administrator is prompted to configure the FortiGate to join the Security Fabric.
3. On the root FortiGate, the new FortiGate must be authorized before it can join the Security Fabric.



If the network contains switches or routers, LLDP may not function as expected because some devices do not pass LLDP packets.

Device request

A device can request to join the Security Fabric from another FortiGate, but it must have the IP address of the root FortiGate. The administrator of the root FortiGate must also authorize the device before it can join the Security Fabric.

The root FortiGate must have FortiTelemetry enabled on the interface that the device connects to.

To enable FortiTelemetry on an interface:

1. Go to *Network > Interfaces*.
2. Edit the interface that the device that you authorizing to join the Security Fabric is connected to.
3. Under *Administrative Access*, enable *Security Fabric Connection*.
4. Under *Network*, turn on *Device Detection*.

To join the Security Fabric by device request:

1. Connect to the unauthorized FortiGate or FortiWiFi device, and go to *Security Fabric > Settings*.
2. Enable *FortiGate Telemetry*.
3. To connect, set *Security Fabric role* to *Join Existing Fabric*.
4. Set *Upstream FortiGate IP* to the IP address of the upstream FortiGate.
5. Connect to the root FortiGate and go to *Security Fabric > Settings*. The new FortiGate appears in the *Topology* as unauthorized.
6. Click on the unauthorized device and select *Authorize* to authorize the device.

CLI commands

Use the following commands to view, accept, and deny authorization requests, to view upstream and downstream devices, and to list or test fabric devices:

Command	Description
diagnose sys csf authorization pending-list	View pending authorization requests on the root FortiGate.
diagnose sys csf authorization accept <serial-number-value>	Authorize a device to join the Security Fabric.
diagnose sys csf authorization deny <serial-number-value>	Deny a device from joining the Security Fabric.
diagnose sys csf downstream	Show connected downstream devices.
diagnose sys csf upstream	Show connected upstream devices.
diagnose sys csf fabric-device list	List all known fabric devices.
diagnose sys csf fabric-device test	Test connections to locally configured fabric devices.

Desynchronizing settings

By default, the settings for FortiAnalyzer logging, central management, sandbox inspection, and FortiClient EMS are synchronized between all FortiGate devices in the Security Fabric. To disable the automatic synchronization of these settings, use the following CLI command:

```
config system csf
  set configuration-sync local
end
```

Deauthorizing a device

A device can be deauthorized to remove it from the Security Fabric.

To deauthorize a device:

1. On the root FortiGate, go to *Security Fabric > Settings*
2. In the Topology field, click on the device and select *Deauthorize*.
3. Click on the device.

After devices are deauthorized, the devices' serial numbers are saved in a trusted list that can be viewed in the CLI using the `show system csf` command. For example, this result shows a deauthorized FortiSwitch:

```
show system csf
config system csf
  set status enable
  set group-name "Office-Security-Fabric"
  set group-password ENC 1Z2X345V678
  config trusted-list
    edit "FGT6HD391806070"
    next
    edit "S248DF3X17000482"
    set action deny
  next
end
end
end
```

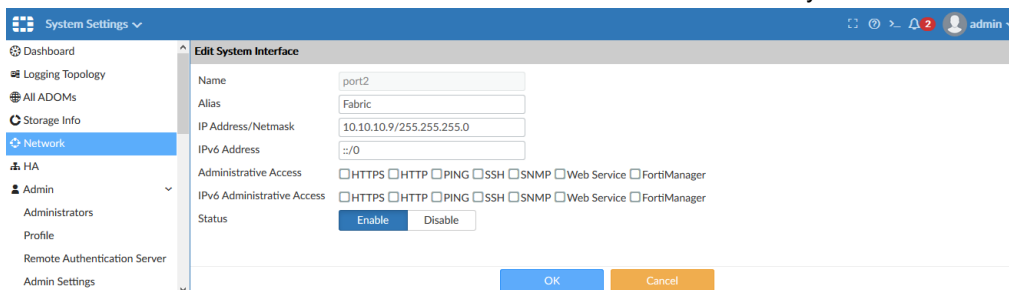
Configuring FortiAnalyzer

FortiAnalyzer is a required component for the Security Fabric. It allows the Security Fabric to show historical data for the Security Fabric topology and logs for the entire Security Fabric.

For more information about using FortiAnalyzer, see the [FortiAnalyzer Administration Guide](#).

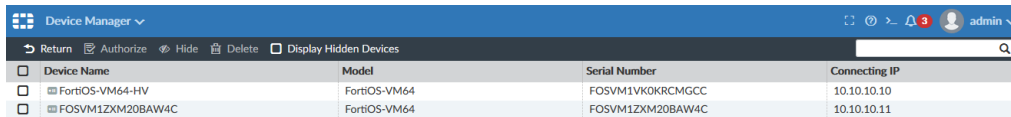
To connect a FortiAnalyzer to the Security Fabric:

1. Enable *FortiAnalyzer Logging* on the root FortiGate. See [Configure the root FortiGate on page 71](#).
2. On the FortiAnalyzer, go to *System Settings > Network* and click *All Interfaces*.
3. Edit the port that connects to the root FortiGate.
4. Set the *IP Address/Netmask* to the IP address that is used for the Security Fabric on the root FortiGate.



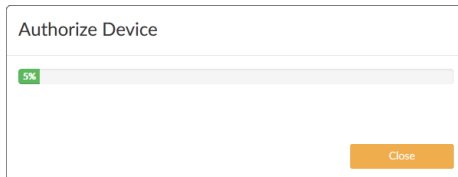
5. Click **OK**.
If the FortiGates have already been configured, it will now be listed as an unauthorized device.

6. Go to *Device Manager > Devices Unauthorized*. The unauthorized FortiGate devices are listed.

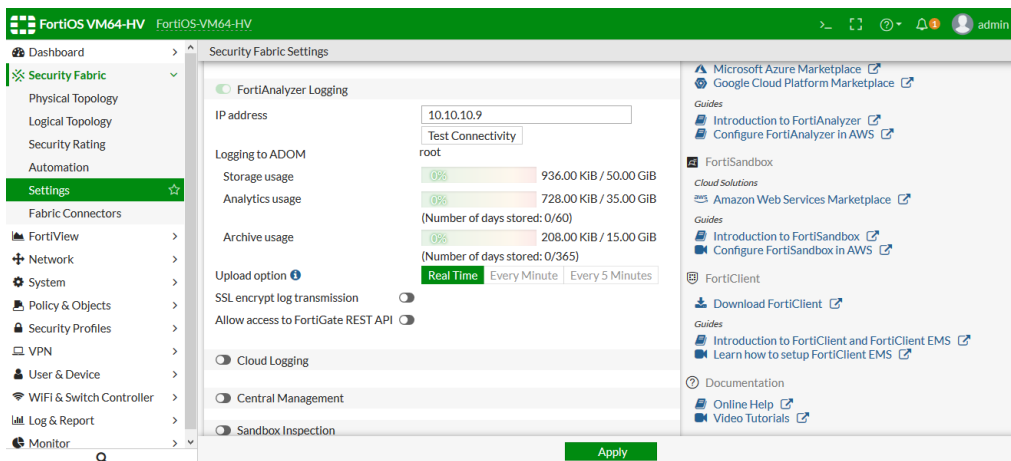


Device Name	Model	Serial Number	Connecting IP
FortiOS-VM64-HV	FortiOS-VM64	FOSVM1VK0KRCMGCC	10.10.10.10
FOSVM1ZXM20BAW4C	FortiOS-VM64	FOSVM1ZXM20BAW4C	10.10.10.11

7. Select the root FortiGate and downstream FortiGate devices in the list, then click *Authorize*. The *Authorize Device* page opens.
8. Click *OK* to authorize the selected devices.



On the FortiGate devices, the *FortiAnalyzer Logging* section on the *Security Fabric > Settings* page will now show the ADOM on the FortiAnalyzer that the FortiGate is in, and the storage, analytics, and archive usage.



Configuring other Security Fabric devices

This section contains information about configuring the following devices as part of the Fortinet Security Fabric:

- [FortiAnalyzer Cloud service on page 77](#)
- [FortiManager on page 81](#)
- [FortiManager Cloud service on page 81](#)
- [FortiSandbox on page 83](#)
- [FortiClient EMS on page 85](#)
- [FortiAP and FortiSwitch on page 88](#)
- [Additional devices on page 88](#)

Prerequisites

- FortiGate devices must either have VDOMs disabled or be running in split-task VDOM mode in order to be added to the Security Fabric. See [Virtual Domains on page 650](#).
- FortiGate devices must be operating in NAT mode.

FortiAnalyzer Cloud service

FortiGate supports the FortiAnalyzer Cloud service for event logging.



Traffic and security logs are not supported in the initial version of FortiAnalyzer Cloud.

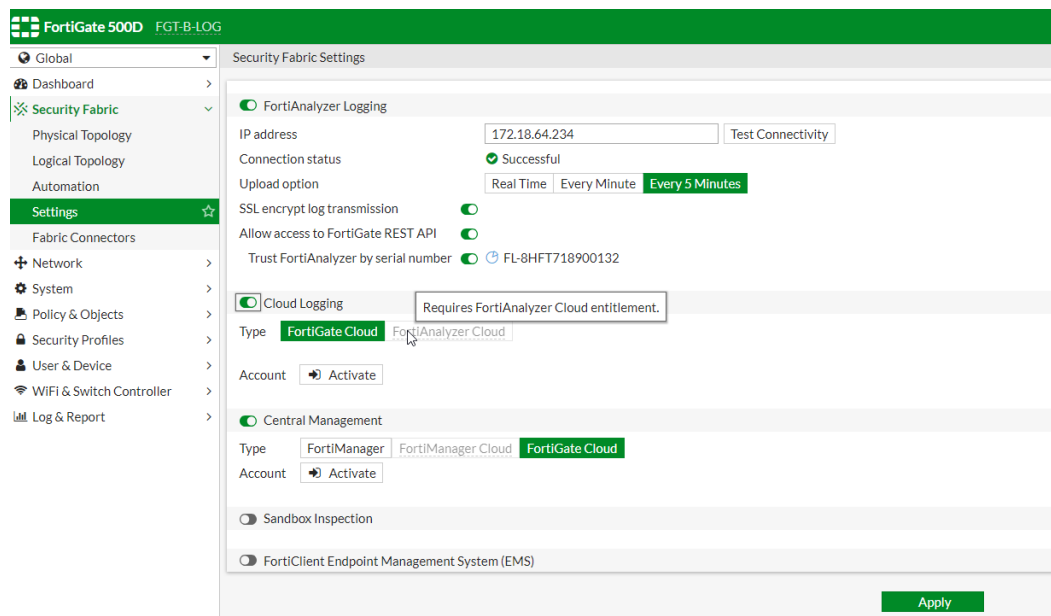
When FortiAnalyzer Cloud is licensed and enabled (see [Deploying FortiAnalyzer Cloud](#) for more information), all event logs are sent to FortiAnalyzer Cloud by default. All traffic logs, security logs, and archive files are not sent to FortiAnalyzer Cloud.

FortiAnalyzer Cloud differs from FortiAnalyzer in the following ways:

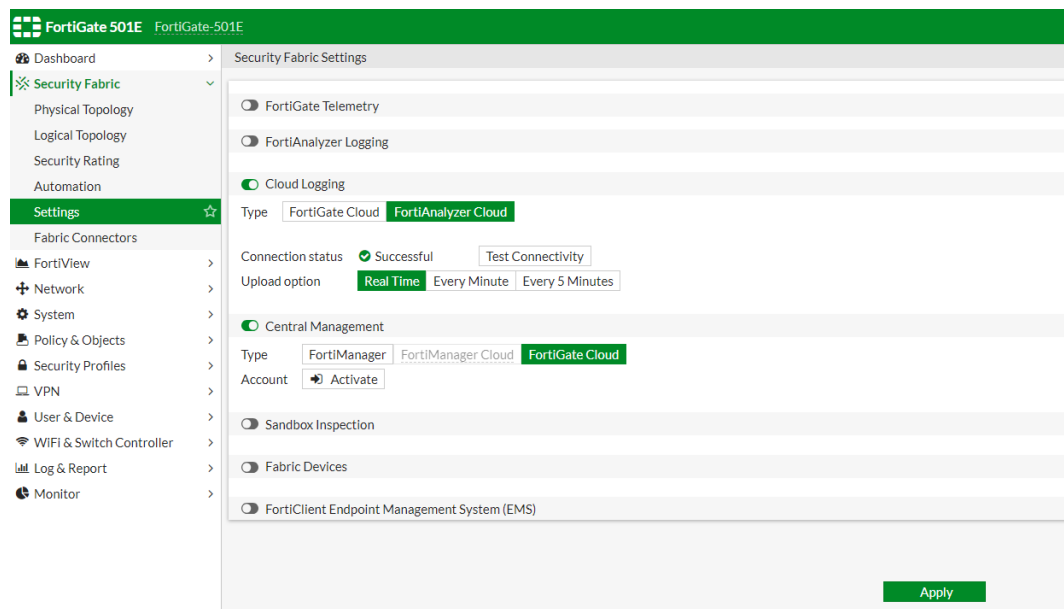
- You cannot enable FortiAnalyzer Cloud in `vdom override-setting` when global FortiAnalyzer Cloud is disabled.
- You must use the CLI to retrieve and display logs sent to FortiAnalyzer Cloud. The FortiOS GUI is not supported.
- You cannot enable FortiAnalyzer Cloud and FortiGate Cloud at the same time.

Sample settings panes

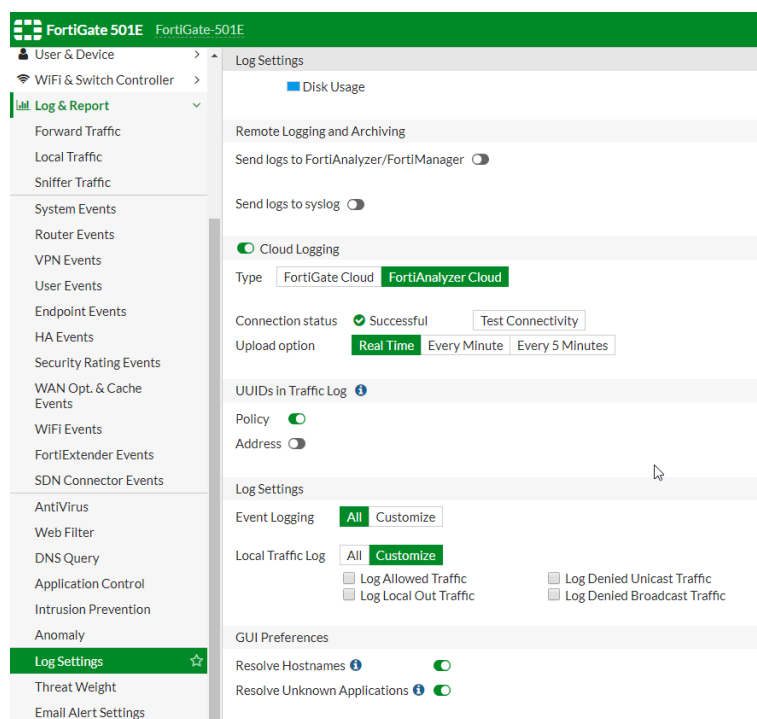
In the FortiOS *Security Fabric* > *Settings* pane under *Cloud Logging*, *FortiAnalyzer Cloud* is grayed out when you do not have a FortiAnalyzer Cloud entitlement.



When you have a FortiAnalyzer Cloud entitlement, *FortiAnalyzer Cloud* is available.



You can also view the FortiAnalyzer Cloud settings in the *Log & Report > Log Settings* pane.



In FortiAnalyzer Cloud, you can view logs from *FortiOS* in the *Event > All Types* pane.

#	Date/Time	Level	Device ID	Action	Message	User	User Interface
1	10:52:45	alert	FGSH1E5818900076		Configuration is changed in the admin session	admin	ssh(10.6.30.254)
2	05-01 18:07	alert	FGSH1E5818900076		Configuration is changed in the admin session	admin	ssh(10.6.30.254)
3	05-01 18:00	alert	FGSH1E5818900076		Configuration is changed in the admin session	admin	ssh(10.6.30.254)
4	05-01 17:57	alert	FGSH1E5818900076	login	Administrator ddd login failed from https10...	ddd	https(10.6.30.254)
5	05-01 17:57	information	FGSH1E5818900076	Edit	Edit log fortianalyzer-cloud filter	admin	ssh(10.6.30.254)
6	05-01 17:56	information	FGSH1E5818900076	Edit	Edit log setting	admin	ssh(10.6.30.254)
7	05-01 17:56	notice	FGSH1E5818900076	connect	Connected to FortiAnalyzer fortianalyzer.for...		
8	05-01 17:55	alert	FGSH1E5818900076	login	Administrator ccc login failed from https10.6...	ccc	https(10.6.30.254)
9	05-01 17:55	alert	FGSH1E5818900076	login	Administrator bbb login failed from https10...	bbb	https(10.6.30.254)
10	05-01 17:53	alert	FGSH1E5818900076	login	Administrator aaa login failed from https10.6...	aaa	https(10.6.30.254)
11	05-01 17:53	information	FGSH1E5818900076	Edit	Edit log fortianalyzer-cloud override-filter	admin	ssh(10.6.30.254)
12	05-01 17:53	information	FGSH1E5818900076	logout	Administrator admin timed out on https10.6...	admin	https(10.6.30.254)
13	05-01 17:53	notice	FGSH1E5818900076	perf-stats	Performance statistics: average CPU: 0, mem...		
14	05-01 17:53	information	FGSH1E5818900076		Delete 1 old report files		
15	05-01 17:51	notice	FGSH1E5818900076	connect	Connected to FortiAnalyzer fortianalyzer.for...		
16	05-01 17:48	notice	FGSH1E5818900076	perf-stats	Performance statistics: average CPU: 0, mem...		
17	05-01 17:48	information	FGSH1E5818900076		Delete 1 old report files		
18	05-01 17:48	information	FGSH1E5818900076		Delete 2 old report files		
19	05-01 17:45	information	FGSH1E5818900076	login	Administrator admin logged in successfully fr...	admin	https(10.6.30.254)
20	05-01 17:45	notice	FGSH1E5818900076	connect	Connected to FortiAnalyzer fortianalyzer.for...		
21	05-01 17:33	information	FGSH1E5818900076		Delete 1 old report files		
22	05-01 17:21	information	FGSH1E5818900076	Edit	Edit log setting	admin	ssh(10.6.30.254)
23	05-01 17:20	information	FGSH1E5818900076	login	Administrator admin logged in successfully fr...	admin	https(10.6.30.254)
24	05-01 17:20	information	FGSH1E5818900076	login	Administrator admin logged in successfully fr...	admin	ssh(10.6.30.254)
25	05-01 17:20	information	FGSH1E5818900076		FS224D3214000736 Discovered	Switch-Controller	fortilinkd
26	05-01 17:20	notice	FGSH1E5818900076	connect	Connected to FortiAnalyzer fortianalyzer.for...		
27	05-01 17:18	information	FGSH1E5818900076	Edit	Edit system.admin admin	admin	GUI(10.6.30.254)
28	05-01 17:18	information	FGSH1E5818900076	Edit	Edit log fortianalyzer-cloud setting	admin	GUI(10.6.30.254)
29	05-01 17:18	notice	FGSH1E5818900076	connect	Connected to FortiAnalyzer fortianalyzer.for...		
30	05-01 17:16	information	FGSH1E5818900076	login	Administrator admin logged in successfully fr...	admin	https(10.6.30.254)
31	05-01 17:14	notice	FGSH1E5818900076		The ntp daemon adjusted time from Wed Ma... Fortilink-FS224D3214000736		

To enable fortianalyzer-cloud using the CLI:

```
config log fortianalyzer-cloud setting
  set status enable
  set ips-archive disable
  set access-config enable
  set enc-algorithm high
  set ssl-min-proto-version default
  set conn-timeout 10
  set monitor-keepalive-period 5
  set monitor-failure-retry-period 5
  set certificate ''
  set source-ip ''
  set upload-option realtime
end
config log fortianalyzer-cloud filter
  set severity information
  set forward-traffic disable
  set local-traffic disable
  set multicast-traffic disable
  set sniffer-traffic disable
  set anomaly disable
  set voip disable
  set dlp-archive disable
  set dns disable
  set ssh disable
  set ssl disable
  set cifs disable
  set filter ''
  set filter-type include
end
```

To disable fortianalyzer-cloud for a specific VDOM using the CLI:

```
config log setting
  set faz-override enable
end
config log fortianalyzer-cloud override-setting
  set status disable
```

```
end
```

To set fortianalyzer-cloud filter for a specific vdom using the CLI:

```
config log setting
    set faz-override enable
end
config log fortianalyzer-cloud override-setting
    set status enable
end
config log fortianalyzer-cloud override-filter
    set severity information
    set forward-traffic disable
    set local-traffic disable
    set multicast-traffic disable
    set sniffer-traffic disable
    set anomaly disable
    set voip disable
    set dlp-archive disable
    set dns disable
    set ssh disable
    set ssl disable
    set cifs disable
    set filter ''
    set filter-type include
end
```

To display fortianalyzer-cloud log using the CLI:

```
execute log filter device fortianalyzer-cloud
execute log filter category event
execute log display
```

Sample log

```
date=2019-05-01 time=17:57:45 idseq=60796052214644736 bid=100926 dvid=1027 itime="2019-05-01
17:57:48" euid=3 epid=3 dsteuid=0 dstepid=3 logver=602000890 logid=0100032002
type="event" subtype="system" level="alert" srcip=10.6.30.254 dstip=10.6.30.9
action="login" msg="Administrator ddd login failed from https(10.6.30.254) because of
invalid user name" logdesc="Admin login failed" sn="0" user="ddd" ui="https
(10.6.30.254)" status="failed" reason="name_invalid" method="https"
eventtime=1556758666274548325 devid="FG5H1E5818900076" vd="root" dtime="2019-05-01
17:57:45" itime_t=1556758668 devname="FortiGate-501E"
date=2019-05-01 time=17:57:21 idseq=60796052214644736 bid=100926 dvid=1027 itime="2019-05-01
17:57:23" euid=3 epid=3 dsteuid=0 dstepid=3 logver=602000890 logid=0100044546
type="event" subtype="system" level="information" action="Edit" msg="Edit
log.fortianalyzer-cloud.filter " logdesc="Attribute configured" user="admin" ui="ssh
(10.6.30.254)" cfgtid=164757536 cfgpath="log.fortianalyzer-cloud.filter"
cfgattr="severity[information->critical]" eventtime=1556758642413367644
devid="FG5H1E5818900076" vd="root" dtime="2019-05-01 17:57:21" itime_t=1556758643
devname="FortiGate-501E"
```

FortiManager

When a FortiManager device is added to the Security Fabric, it automatically synchronizes with any connected downstream devices.

To add a FortiManager to the Security Fabric, configure central management on the root FortiGate. The root FortiGate then pushes this configuration to downstream FortiGate devices. The FortiManager provides remote management of FortiGate devices over TCP port 541. The FortiManager must have internet access for it to join the Security Fabric.

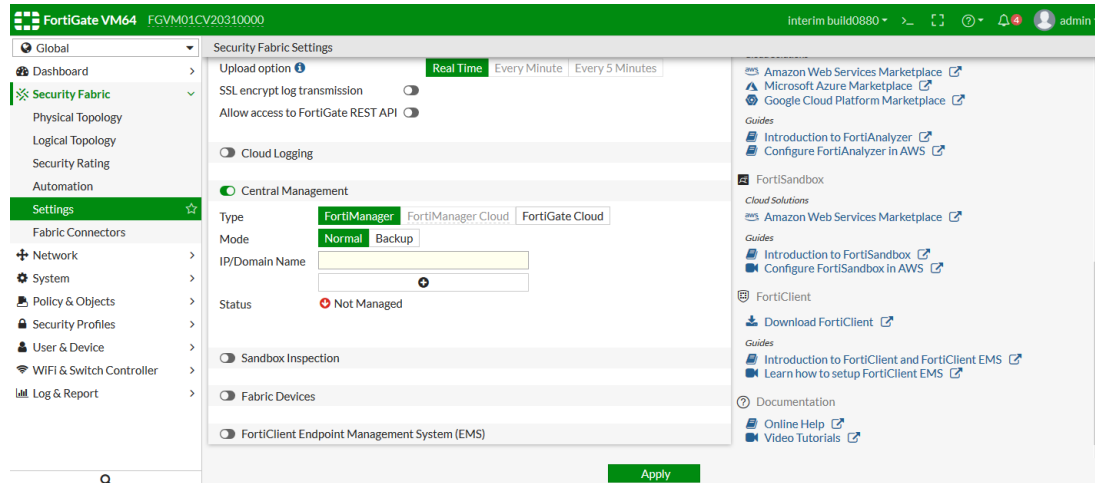
Once configured, the FortiGate can receive antivirus and IPS updates, and allow remote management through FortiManager or the FortiGate Cloud service. The FortiGate management option must be enabled so that the FortiGate can accept management updates to its firmware and FortiGuard services.

To add a FortiManager to the Security Fabric using the CLI:

```
config system central-management
  set type fortimanager
  set fmg {<IP_address> | <FQDN_address>}
end
```

To add a FortiManager to the Security Fabric using the GUI:

1. On the root FortiGate, go to *Security Fabric > Settings*.
2. Enable *Central Management*.
3. Set the *Type* to *FortiManager*.



4. Enter the *IP/Domain Name* of the FortiManager.
 5. Click *Apply*.
 6. On the FortiManager, go to *Device Manager* and find the FortiGate in the *Unauthorized Devices* list.
 7. Select the FortiGate device or devices, and click *Authorize* in the toolbar.
 8. In the *Authorize Device* pop-up, adjust the device names as needed, then click *OK*.
- For more information about using FortiManager, see the [FortiManager Administration Guide](#).

FortiManager Cloud service

This cloud-based SaaS management service is available through FortiManager.

Once the FortiGate has acquired a contract named *FortiManager Cloud*, FortiCloud creates a cloud-based FortiManager instance under the user account. You can launch the portal for the cloud-based FortiManager from FortiCloud, and its URL starts with the User ID.

You can use a FortiGate with a contract for *FortiManager Cloud* to configure central management by using the FQDN of *fortimanager.forticloud.com*. A FortiGate-FortiManager tunnel is established between FortiGate and the FortiManager instance.

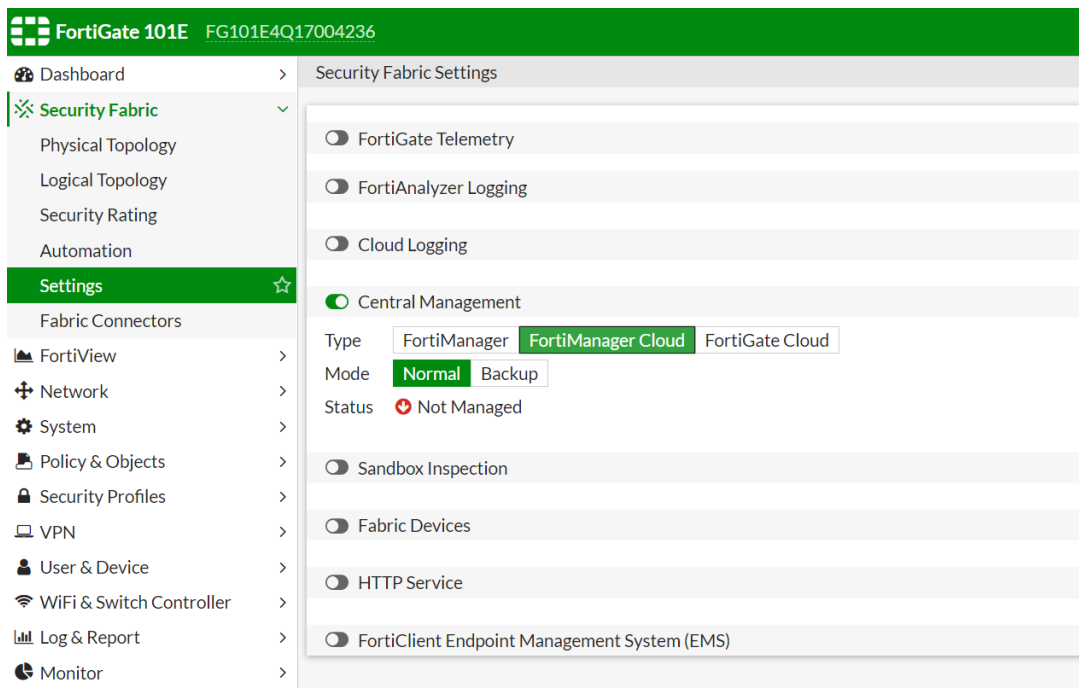
After the tunnel is established, you can execute FortiManager functions from the cloud-based FortiManager portal.

To configure FortiManager Cloud central management:

1. Enable FortiManager Cloud:
 - a. Go to *Security Fabric > Settings*.
 - b. Enable *Central Management*.
 - c. Click *FortiManager Cloud*.
 - d. Click *Apply*.



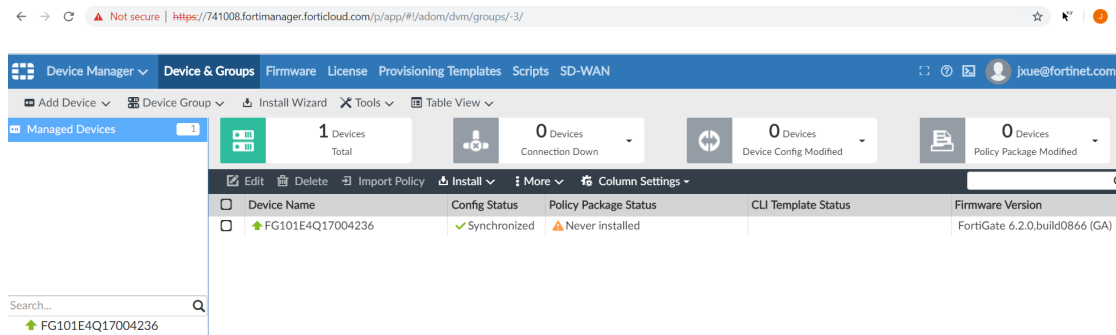
The *FortiManager Cloud* button can only be selected if you have a FortiManager Cloud product entitlement.



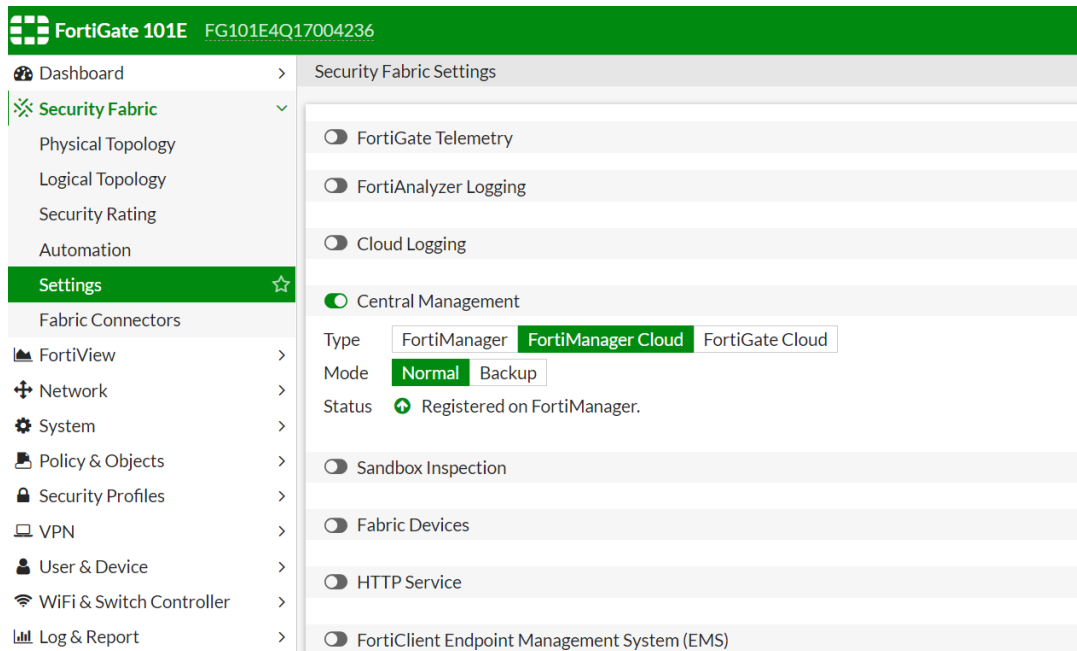
2. In the FortiManager Cloud instance, go to *Device Manager* and authorize the FortiGate. See [Authorizing devices](#) for more information.
When using FortiGate to enable FortiManager Cloud, the FortiGate appears as an unauthorized device.



After authorizing the FortiGate, it becomes a managed device.



In FortiOS, the *Central Management Status* now displays as *Registered on FortiManager*.



FortiSandbox

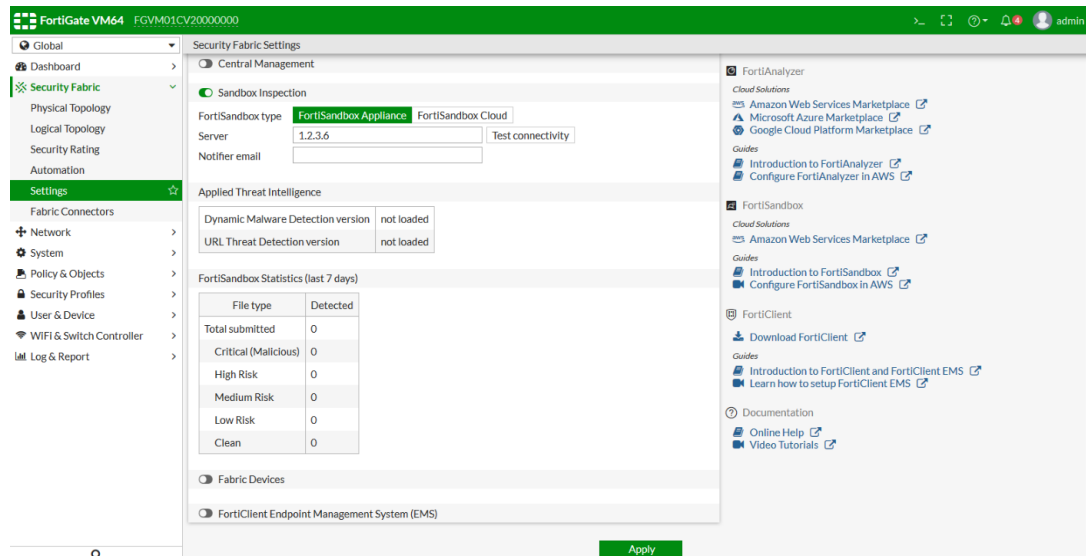
The Security Fabric supports FortiSandbox appliances and FortiSandbox Cloud. A FortiGate Cloud account is not required.

To use FortiSandbox in a Security Fabric, connect the FortiSandbox to the Security Fabric, then configure an antivirus profile to send files to the FortiSandbox. Sandbox inspection can also be used in Web Filter profiles.

FortiSandbox settings are configured on the root FortiGate of the Security Fabric. After configuration, the root FortiGate pushes the settings to other FortiGate devices in the Security Fabric.

To add a FortiSandbox appliance to the Security Fabric:

1. On the root FortiGate, go to *Security Fabric > Settings*.
2. Enable *Sandbox Inspection* and set the *FortiSandbox Type* to *FortiSandbox Appliance*.
3. In the *Server* field, enter the FortiSandbox device's IP address.



4. Optionally, enter a *Notifier email*.
5. Click *Apply*.
6. On the FortiSandbox appliance, go to *Scan Input > Device*.
7. Edit the root FortiGate.
8. Under *Permissions*, check the *Authorized* box.
9. Click *OK*.
10. Authorize the rest of the FortiGate devices that are in the Security Fabric.

To add a FortiSandbox Cloud instance to the Security Fabric:

1. On the root FortiGate, go to *Security Fabric > Settings*.
2. Enable *Sandbox Inspection* and set the *FortiSandbox Type* to *FortiSandbox Cloud*.
3. Select the *FortiSandbox cloud region* from the drop-down list. Data from your network will only be sent to servers in the selected region.
4. Click *Apply*.



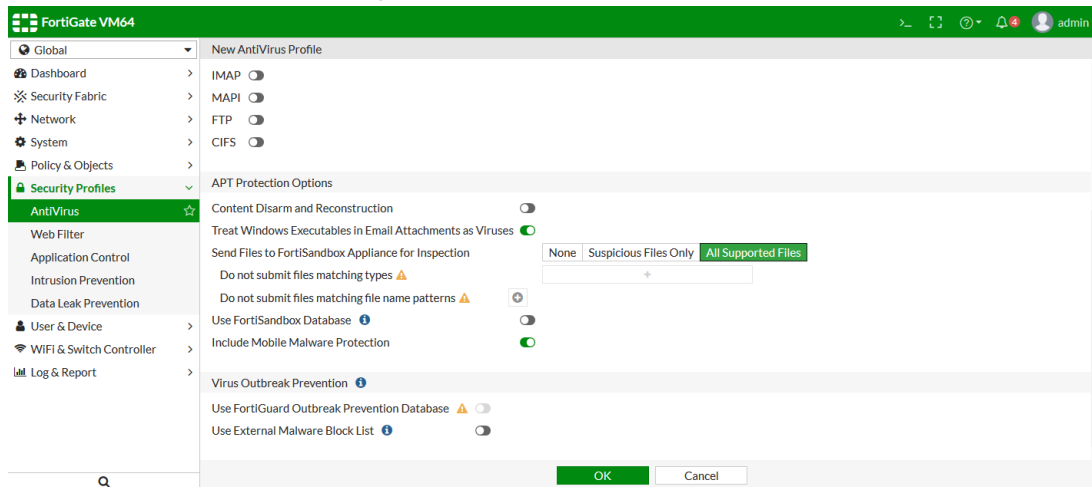
If *FortiSandbox Cloud* is not visible in the GUI, run the `execute forticloud-sandbox region` and `execute forticloud-sandbox update` commands.

Antivirus profiles

An antivirus profile must be configured to send files to the FortiSandbox.

To configure an antivirus profile:

1. On the FortiGate, go to *Security Profile > AntiVirus*.
2. Create, edit, or clone an antivirus profile.



3. Under *APT Protection Options*, set *Send Files to FortiSandbox Appliance for Inspection* to *All Supported Files*.
4. Optionally, configure file exceptions.
5. Enable *Use FortiSandbox Database*.
6. Click **OK**.

Web Filter profiles

Sandbox inspection can be used in Web Filter profiles.

To configure a Web Filter profile:

1. On the FortiGate, go to *Security Profiles > Web Filter*.
2. Create, edit, or clone a profile.
3. Under *Static URL Filter*, enable *Block malicious URLs discovered by FortiSandbox*.
4. Click **OK**.

FortiClient EMS

The FortiGate Security Fabric root device can link to FortiClient Endpoint Management System (EMS) and FortiClient EMS Cloud (a cloud-based EMS solution) for endpoint connectors and automation. Up to three EMS servers can be added on the global Security Fabric settings page, including on FortiClient EMS Cloud server. EMS settings are synchronized between all fabric members.

To enable cloud-based EMS services, FortiGate must be registered to FortiCloud with an appropriate user account.



If you disable *FortiClient Endpoint Management System (EMS)* on the *Security Fabric > Settings* page, all previously configured EMS server entries will be deleted.

To add a FortiClient EMS server to the Security Fabric in the CLI:

```
config endpoint-control fctems
  edit <ems_name>
    set server <ip_address>
    set serial-number <string>
    set admin-username <string>
    set admin-password <string>
    set https-port <integer>
    set source-ip <ip_address>
  next
end
```

The `https-port` is the EMS HTTPS access port number, and the `source-ip` is the REST API call source IP address.

To add a FortiClient EMS Cloud server to the Security Fabric in the CLI:

1. Enable authentication of FortiClient EMS Cloud through a FortiCloud account:

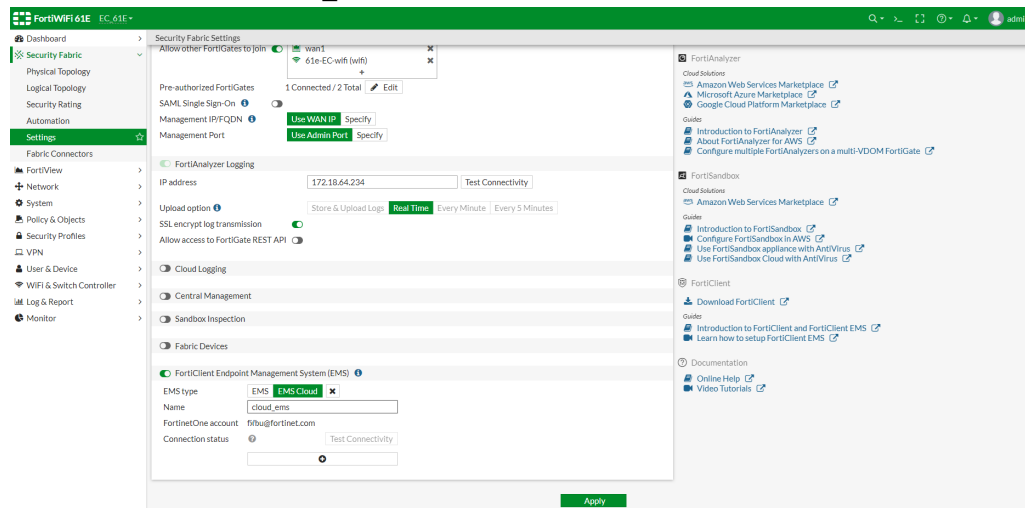
```
config endpoint-control fctems
  edit <name>
    set fortinetone-cloud-authentication enable
  next
end
```

2. Create a FortiClient EMS Cloud server connection:

```
config user fsso
  edit "cloud_ems_fsso_connector"
    set type fortiems-cloud
    set password *****
    set source-ip <class_ip>
  next
end
```

To add both a cloud-based and an on-premise FortiClient EMS server to the Security Fabric in the GUI:

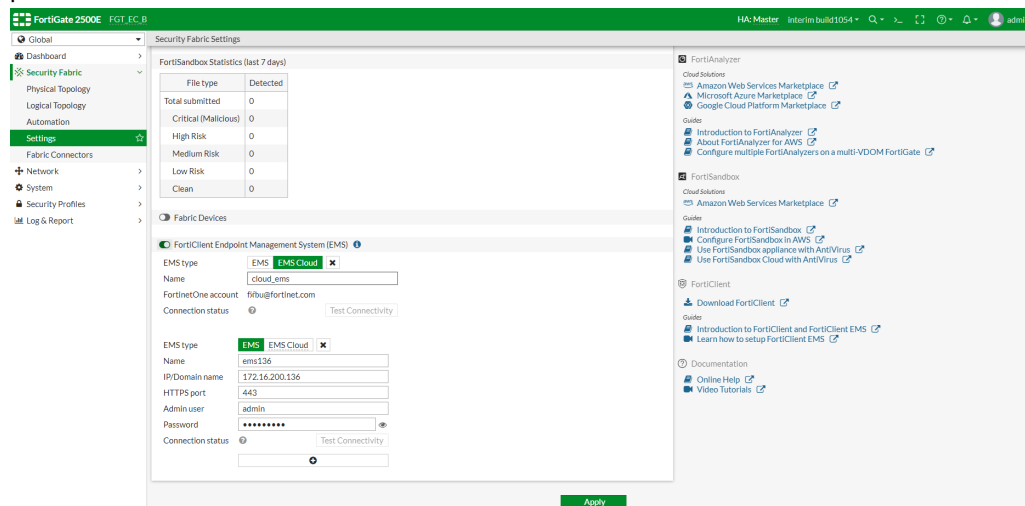
1. To enable endpoint control, on the root FortiGate, go to *System > Feature Visibility* and enable *Endpoint Control*.
2. Go to *Security Fabric > Settings*.
3. Enable *FortiClient Endpoint Management System (EMS)*.
4. Add an EMS server.
5. Set *EMS Type* to *EMS Cloud*.

6. Enter a name, such as *cloud_ems*.

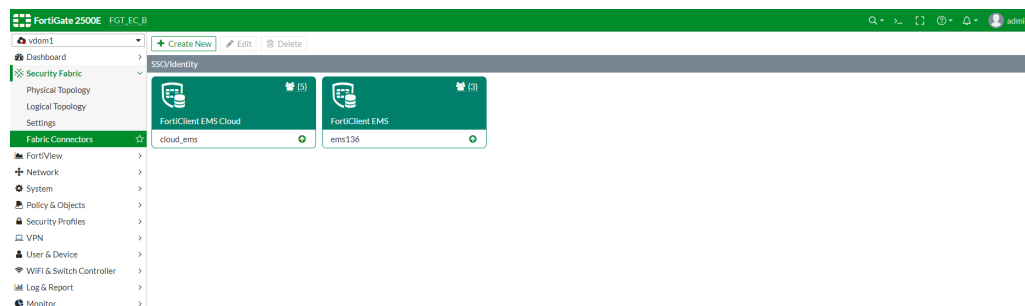
7. Add another EMS server.

8. Set *EMS Type* to *EMS*.9. Enter a name, such as *ems136*.

10. Enter server's IP address, admin user name, and admin password. Optionally, you can also change the HTTPS port.

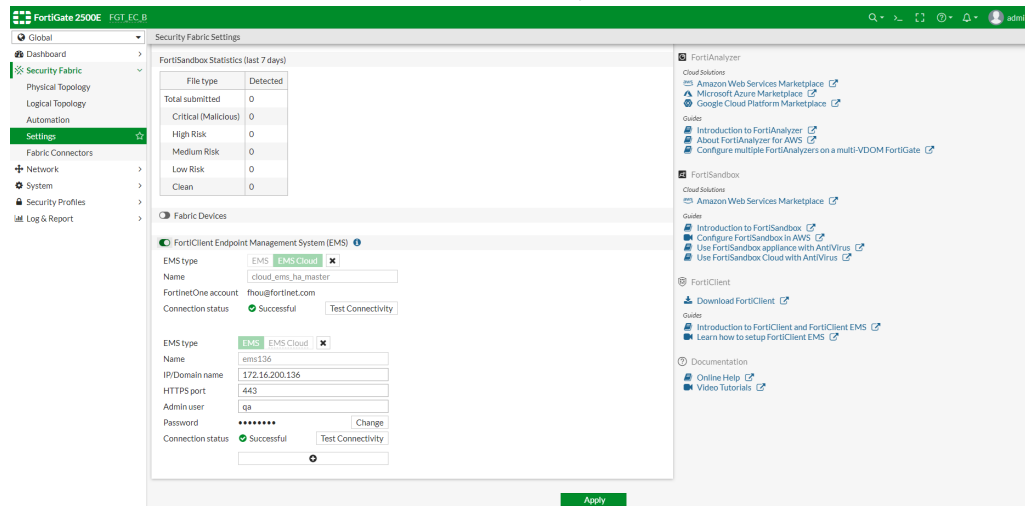
11. Click *Apply*.

FortiClient EMS fabric connectors are automatically created for the EMS servers.



To test connectivity with the EMS server:

1. Go to *Security Fabric > Settings* and go to the *FortiClient Endpoint Management System (EMS)* section.
2. In the *Connection status* field, click *Test Connectivity*.



FortiAP and FortiSwitch

FortiAP and FortiSwitch devices can be authorized in the Security Fabric with one click. After connecting a FortiAP or FortiSwitch device to an authorized FortiGate, it will automatically be listed in the topology tree.



If the default `auto-auth-extension-device` settings on the FortiAP or FortiSwitch have been modified, manual authorization in the Security Fabric may not be required.

For more information about configuring FortiAPs, see [Configuring the FortiGate interface to manage FortiAP units](#) and [Discovering, authorizing, and deauthorizing FortiAP units](#).

For more information about configuring FortiSwitches, see [Using the FortiGate GUI](#).

To authorize FortiAP and FortiSwitch devices:

1. Connect the FortiAP or FortiSwitch device to a FortiGate.
2. On the root FortiGate, go to *Security Fabric > Settings*. The new device will be shown in the *Topology*.
3. Click on the device and select *Authorize*.

Additional devices

The following Fortinet devices are supported by the Security Fabric:

- FortiADC
- FortiDDoS
- FortiSandbox
- FortiMail

- FortiWeb
- FortiWLC

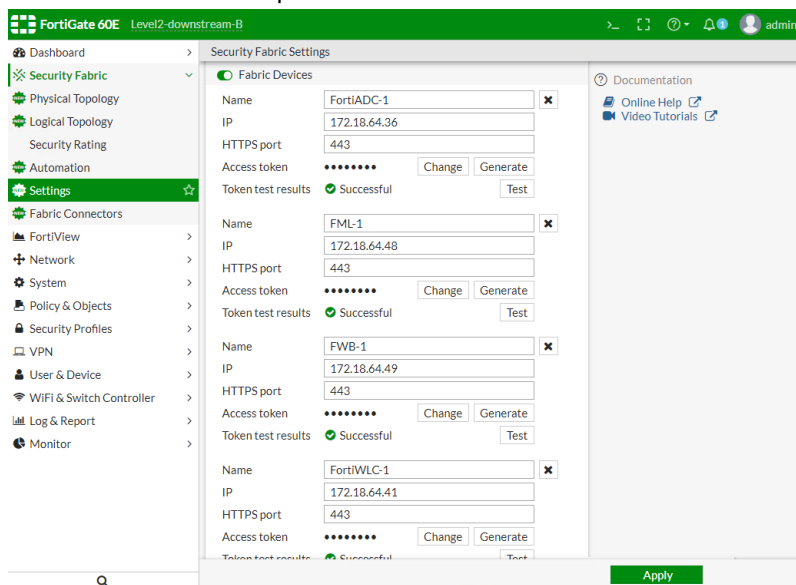


Security Fabric supports standalone FortiSandbox devices, FortiSandbox HA-Cluster primary, and FortiSandbox cluster IP.

In FortiOS, the device details can be shown in *Security Fabric* and *Fabric Device* dashboard widgets, as well as in the Security Fabric settings, and physical and logical topologies.

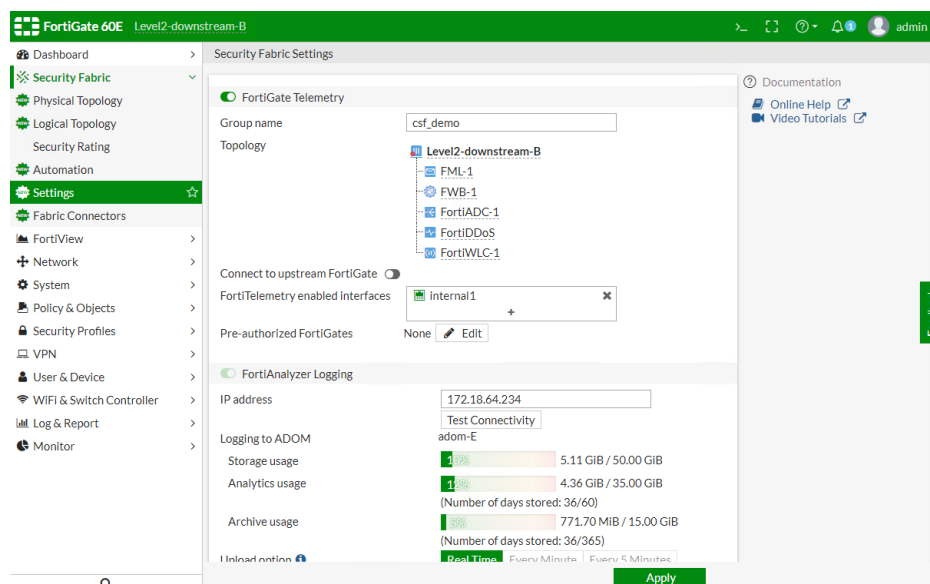
To add one or more of the devices to the Security Fabric in the GUI:

1. On the root FortiGate, go to *Security Fabric > Settings*.
2. Enable *Fabric Devices*.
3. Enter the *Name*, *IP*, *HTTPS port* for the device.
4. Click *Generate* to generate an access token. The *Generate Access Token* pane opens.
 - a. Enter the device's username and password.
 - b. Click *OK*.
5. Add more devices as required.



FortiSandbox only supports HTTPS port 443.

6. Click *Apply*.
The added devices are shown in the *FortiGate Telemetry* section *Topology* list.



To add one or more of the devices to the Security Fabric in the CLI:

```
config system csf
...
config fabric-device
    edit "FortiADC-1"
        set device-ip 172.18.64.36
        set access-token xxxxxx
    next
    edit "FML-1"
        set device-ip 172.18.64.48
        set access-token xxxxxx
    next
    edit "FWB-1"
        set device-ip 172.18.64.49
        set access-token xxxxxx
    next
end
end
```

Using the Security Fabric

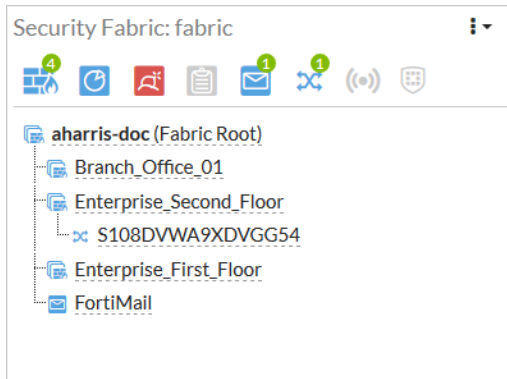
Dashboard widgets

Security Fabric widgets can be added to FortiGate dashboards, including:

- [Security Fabric status on page 91](#)
- [Security Rating on page 91](#)
- [Fabric Device on page 92](#)
- [FortiGate Cloud on page 93](#)

Security Fabric status

The Security Fabric status widget shows a summary of the devices in the Security Fabric.



Hover the cursor over the top icons to view pop-ups showing the statuses of the devices in the fabric.

The device tree shows devices that are connected, or could be connected, to your Security Fabric, according to the following color scheme:

- Blue: connected to the network
- Gray: not configured or not detected
- Red: no longer connected or not authorized

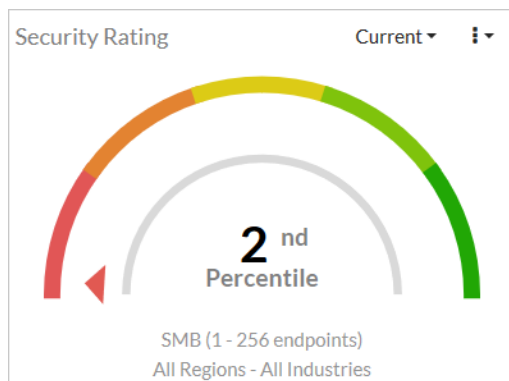
Hover over a device in the tree to view details about the device, such as its serial number, operation mode, IP address, CPU and memory usage, and others, depending on the device type.

Unauthorized FortiAP and FortiSwitch devices are highlighted in the list, and can be authorized by clicking on the device name.

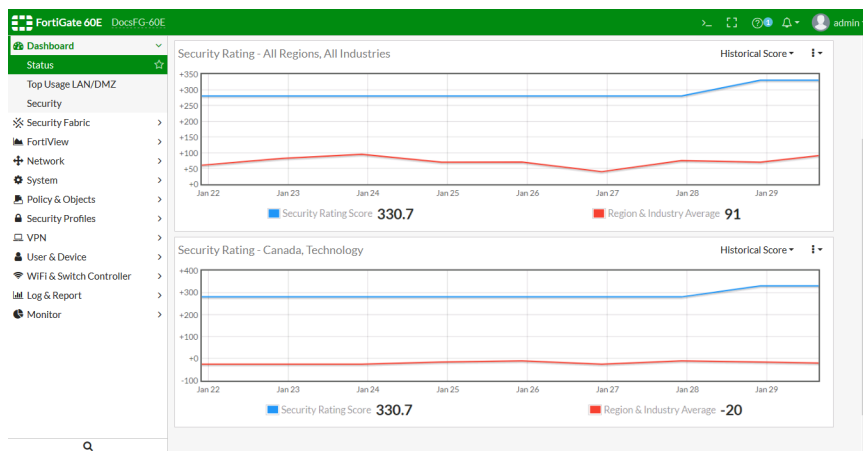
Security Rating

The Security Rating widget shows the security rating for your Security Fabric. It can show the current rating percentile, or historical security rating score or percentile charts.

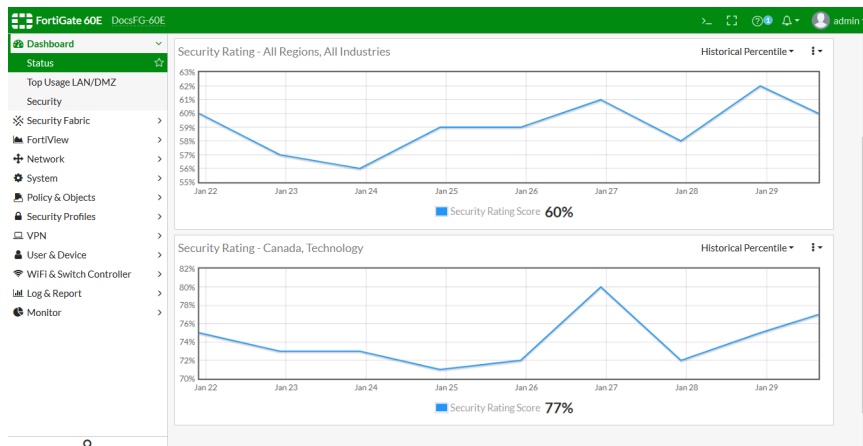
The widget can be configured to show how your organization's security rating compares to the ratings of either all organizations, or only organizations that are in the same industry and/or geographic region as you (determined from your FortiCare account settings).



To switch to the historical security rating score view, select *Historical Score* from the view dropdown menu. Making the widget wider makes the graph easier to read.



To switch to the historical percentile view, select *Historical Percentile* from the view dropdown menu. Making the widget wider makes the graph easier to read.



To receive a security rating score, all FortiGate devices that are in the Security Fabric must have a valid Security Rating License.

Fabric Device

The Fabric Device widget show statistics and system information about the selected fabric device.

For a FortiMail device, the widget can show:

- Mail Statistics: a chart of the total messages and total spam messages over time.
- Statistics Summary: a pie chart summarizes mail statistics.
- System Information: The FortiMail System Information widget
- System Usage: System usage information, such as CPU, memory, and disk usage, as well as the number of active

sessions.

System Usage - FortiMail	
CPU usage	0%
Memory usage	46%
Log disk usage	0%
Mail disk usage	47%
System load	11%
Active sessions	1

FortiGate Cloud

The FortiGate Cloud widget shows the FortiGate Cloud status and information. If your account is not activated, you can activate it from the widget.

FortiGate Cloud	
Status	Activated
Log Retention	Free License
Storage Used	2 GiB
FortiSandbox Cloud	Disabled

To activate your FortiGate Cloud account:

1. Click on the *Not Activated* button and select *Activate*. The *FortiCare Registration* pane opens.

FortiGate-101E FortiGate-101E

FortiGate-101E: FortiCare Registration

Please register with FortiCare before activating FortiGate Cloud.

FortiGate FortiGate-101E

FortiCloud Login Create Account

Email

Password

Forgot your password?

Country/Region

Reseller

Sign in to FortiGate Cloud using the same account

OK Cancel

2. If you already have a FortiCloud account:
 - a. Fill in your email address, password, country or region, and reseller.
 - b. Click OK.
3. If you are creating a FortiCloud account:
 - a. In the *FortiCloud* field select *Create Account*.
 - b. Fill in all of the required information.
 - c. Click OK.

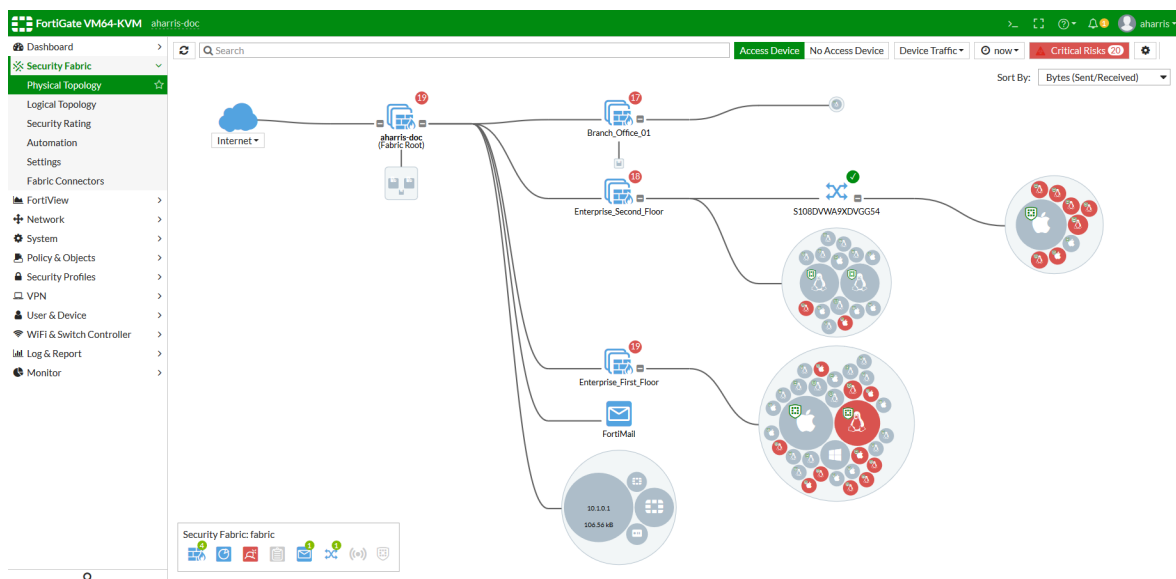
Topology

The full Security Fabric topology can be viewed on the root FortiGate. Downstream FortiGate devices' topology views do not include upstream devices.

The Physical Topology shows the physical structure of your network, including all connected devices and the connections between them. The Logical Topology shows information about the interfaces that connect devices to the Security Fabric. The size of the bubbles in the topology vary based on traffic volume. Only Fortinet devices are shown in the topologies.

In both views, filtering and sorting options allow you to control the information that is shown. Hover the cursor over a device icon, port number, or endpoint to open a tooltip that shows information about that specific device, port, or endpoint. Right-click on a device to log in to it or to deauthorize it. Right-click on an endpoint to perform various tasks, including drilling down for more details on sources or compromised hosts, quarantining the host, and banning the IP address.

The small number that might be shown on the top right corner of a device icon is the number of security ratings recommendations or warnings for that device. The color of the circle shows the severity of the highest security rating check that failed. Clicking on it will open the Security Rating page. See [Security rating on page 133](#) for more information.



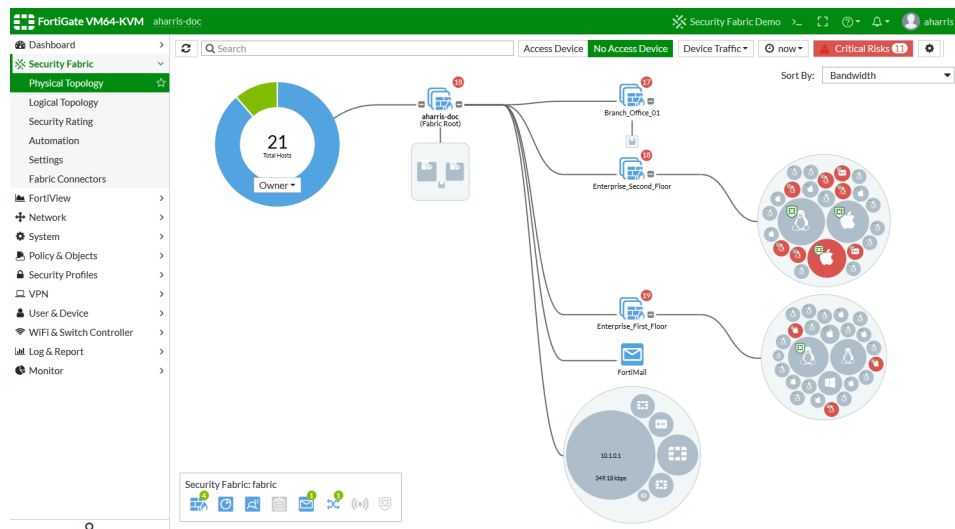
Servers and server clusters are represented by squares with rounded corners, and are grouped separately from circular endpoints. Devices are grouped by device type, and colored based on their risk level.

AWS assets are grouped by AWS security groups or subnets, and information about detected Common Vulnerabilities and Exposures (CVEs), as well as the instance details and ID, are shown.

WAN cloud

The WAN cloud icon includes a drop-down menu for selecting where the destination data comes from. The available options are: *Internet*, *Owner*, *IP Address*, and *Country/Region*. These options are only available when the filtering based on *Device Traffic*.

When *Owner* is selected, the destination hosts are shown as donut charts that show the percentage of internal (with private IP addresses) and Internet hosts. Hover over either color in the chart to see additional information. To see more details, right-click on the chart and select *Destination Owner Details* to go to the *FortiView > Destinations* page.



FortiAP and FortiSwitch devices

Newly discovered FortiAP and FortiSwitch devices are initially shown in the topologies with gray icons to indicate that they have not been authorized. To authorize a device, click on the device icon or name and select *Authorize*. Once authorized, the device icon will turn blue.

Right-click on an authorized FortiAP device to *Deauthorize* or *Restart* the device. Right-click on a FortiSwitch device to *Deauthorize*, *Restart*, or *Upgrade* the device, or to *Connect to the CLI*.

FortiAP and FortiSwitch links are enhanced to show Link Aggregation Groups for the Inter-switch Link (ISL-LAG). To differentiate them from physical links, ISL-LAG links are shown with a thicker line. The endpoint circles can also be used as a reference to identify ISL-LAG groups that have more than two links.

Views

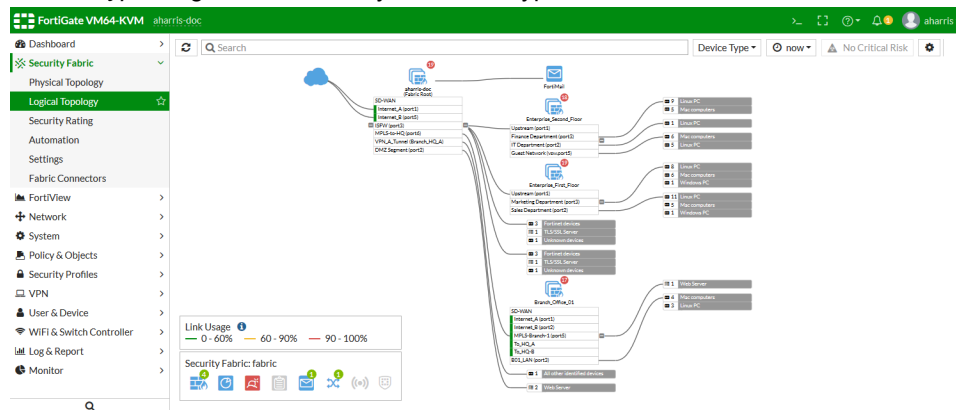
The topology views can be focused using filters and by sorting in different ways to help you locate the information that you need.

Select one of *Access Device* or *No Access Device* to only show access or no access devices in the physical topology.

From the *Bubble Option* drop-down list, select one of the following views:

- *Device Traffic*: Organize devices by traffic.
- *Device Count*: Organize devices by the number of devices connected to it.

- **Device Type:** Organize devices by the device type.

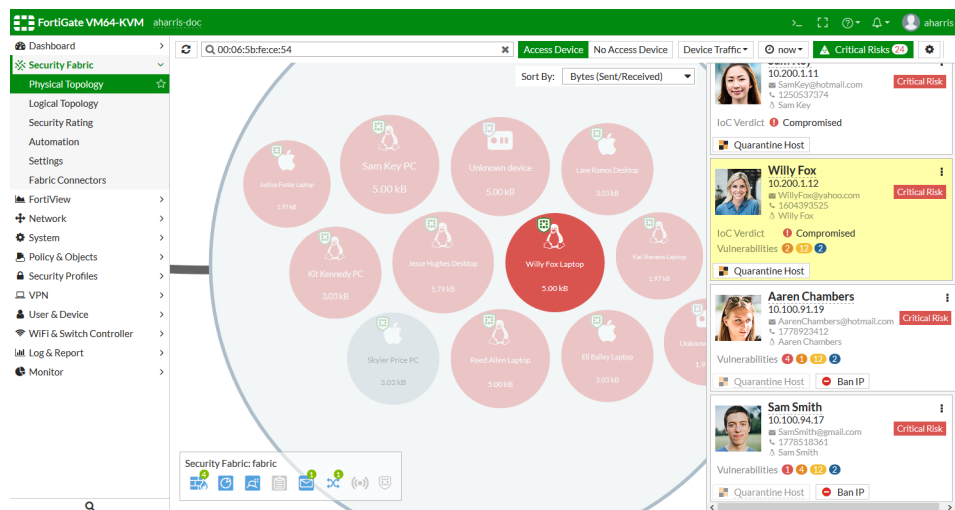


- **Risk:** Only include devices that have endpoints with medium, high, or critical risk values of the specified type: *All, Compromised Host, Vulnerability, Threat Score.*
- **No Devices:** Don't show endpoints.

The time period drop-down list filters the view by time. Options include: *now* (real time), *5 minutes*, *1 hour*, *24 hours*, *7 days*.

Critical risks

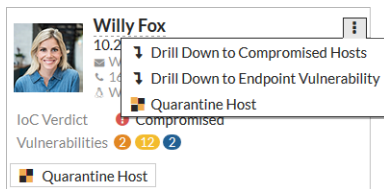
Click the **Critical Risks** button to see a list of endpoints that are deemed critical risks, organized by threat severity. These are the red endpoints in the current topology view.



For each endpoint, the user's photo, name, IP address, email address, and phone number are shown. The number of vulnerabilities of each severity is shown, and if the IOC verdict is that the endpoint is compromised.

If applicable, the endpoint's host can be quarantined or their IP address banned, by clicking the **Quarantine Host** on **Ban IP** button.

The drop-down menu also provides options to drill down to more information on compromised hosts or endpoint vulnerabilities.



Clicking *Drill Down to Compromised Hosts* will open the *FortiView > Compromised Hosts* page showing a summary for the selected endpoint.

Detected Pattern	Threat Type	Threat Name	Threat Type	Detect method	Events	Security Action	Web Category
148.81.111.122	Malware	Sinkhole		Infected-ip	8	close	Unrated
176.31.62.76	Malware	Sinkhole		Infected-ip	8	close	Information Technology
148.81.111.122	Malware	Sinkhole		Infected-ip	7	close	Unrated
176.31.62.76	Malware	Sinkhole		Infected-ip	7	close	Information Technology

Compromised host information can also be viewed on the FortiAnalyzer in *SOC > FortiView > Threats > Compromised Hosts*.



The FortiAnalyzer must have a FortiGuard Indicators of Compromise service license in order to see compromised hosts.

Clicking *Drill Down to Endpoint Vulnerability* will open the vulnerabilities page showing a summary of the vulnerabilities on the selected endpoint.

Vulnerability Name	Severity	Vulnerability Category	CVE-IDs	Vulnerability ID
Mode 6 unauthenticated trap information disclosure and DDos vector	High	Applications	CVE-2016-9311	38950
Origin DoS (Medium)	Medium	Applications	CVE-2016-9042	38951
Bad authentication demobilizes ephemeral associations	Medium	Applications	CVE-2016-4953	38939
Client rate limiting and server responses	Medium	Applications	CVE-2016-7426	38942
Craftedaddpeerwithmode> 7 causes array wraparound withMATCH_ASSOC	Medium	Applications	CVE-2016-2518	38926
NTP-01-004 NTP: Potential Overflows inctl_put(functions (Medium)	Medium	Applications	CVE-2017-6458	38955
NTP-01-012 NTP: Authenticated DoS via Malicious Config Option (Medium)	Medium	Applications	CVE-2017-6463	38960
Original fix for NTP Bug 2901 brokepeerassociations	Medium	Applications	CVE-2015-7704	38922

FortiAnalyzer

The Security Fabric topology can also be seen on the FortiAnalyzer device. In the *Device Manager*, FortiGate devices are shown as part of a Security Fabric group, with an asterisk next to the name of the root FortiGate.

Device Manager

ADOM: Fabric_ADOM

ahilia

4 Devices
Total

0 Devices
Log Status Down

0% Storage Used
Total 30.0 GB

+ Add Device

Edit

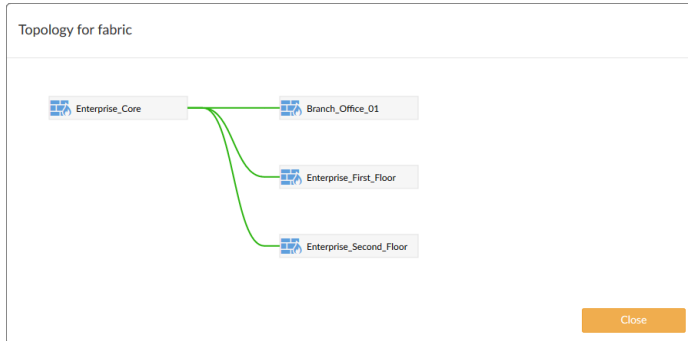
Delete

More

Column Settings

<input type="checkbox"/>	Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)	Device Storage	Description
<input type="checkbox"/>	✖ fabric						
<input type="checkbox"/>	Branch_Office_01	10.1.0.1	FortiGate-VM64	🟢 Real Time	0	(0.01%)	
<input type="checkbox"/>	Enterprise_Core*	10.100.88.1	FortiGate-VM64	🟢 Real Time	0	(0.03%)	
<input type="checkbox"/>	Enterprise_First_Floor	10.100.88.101	FortiGate-VM64	🟢 Real Time	0	(0.03%)	
<input type="checkbox"/>	Enterprise_Second_Floor	10.100.88.102	FortiGate-VM64	🟢 Real Time	0	(0.02%)	

To view the Security Fabric topology, right-click on the fabric group and select *Fabric Topology*. Only Fortinet devices are shown in the Security Fabric topology views.



Topology view — consolidated risk

The topology view shows endpoints based on their highest severity event.

In the default topology view, you can view hosts with critical vulnerabilities and compromised hosts identified as critical risks.

The consolidated *Risk* view mode displays different risks within the Security Fabric topology. You can use the *Risk* view mode to filter threats by *Compromised Hosts*, *Vulnerability*, and *Threat Score*.

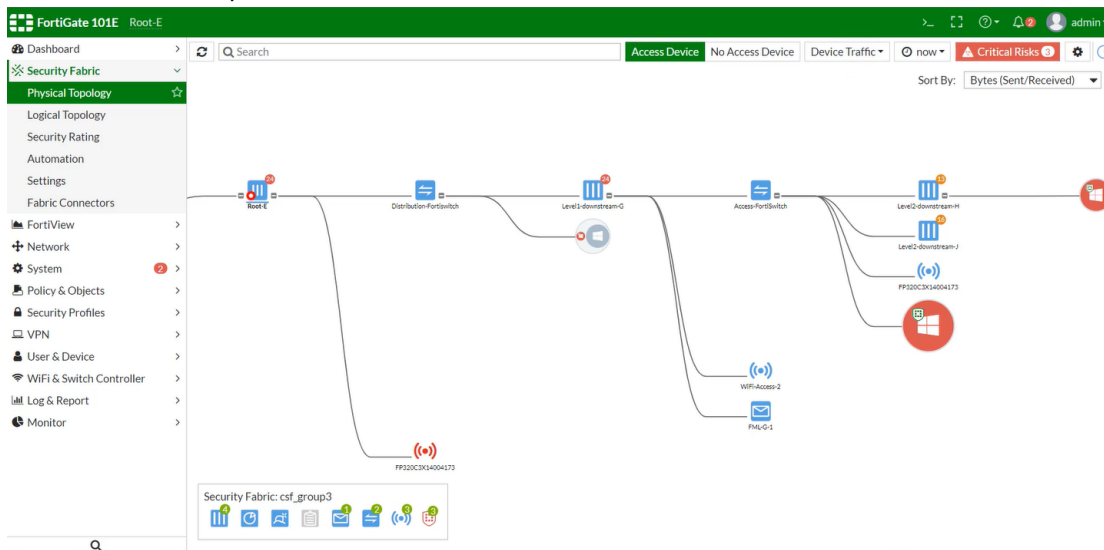


To access the default topology view:

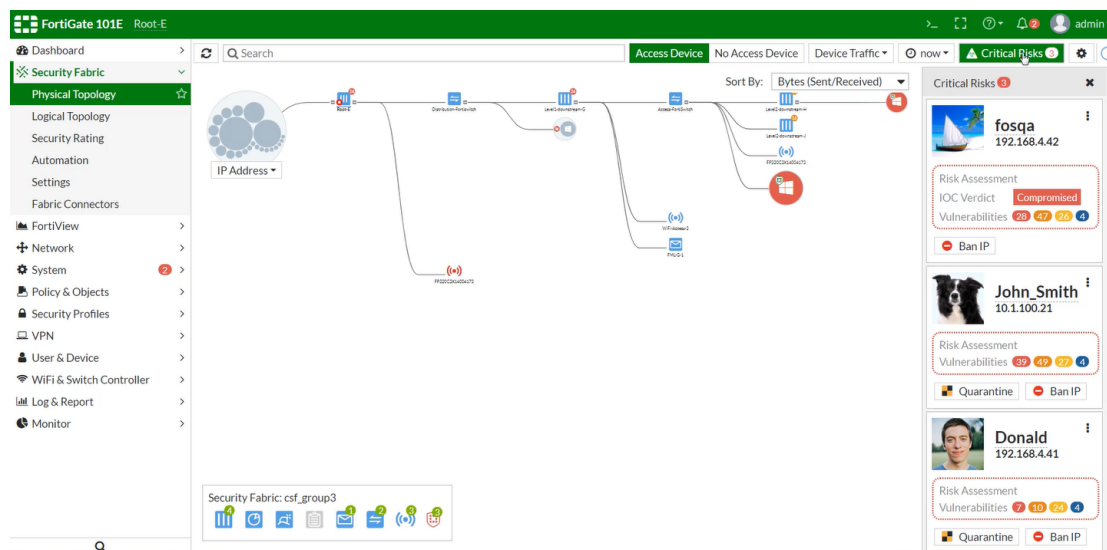
1. Go to *Security Fabric > Physical Topology*.

The default topology view highlights hosts with critical vulnerabilities and compromised hosts as critical risks (three critical risks in the example).

- a. Hover over the tooltips for more details.



2. To view the critical risk summary, click *Critical Risks*.
The *Critical Risks* pane displays on the right-side of the screen.



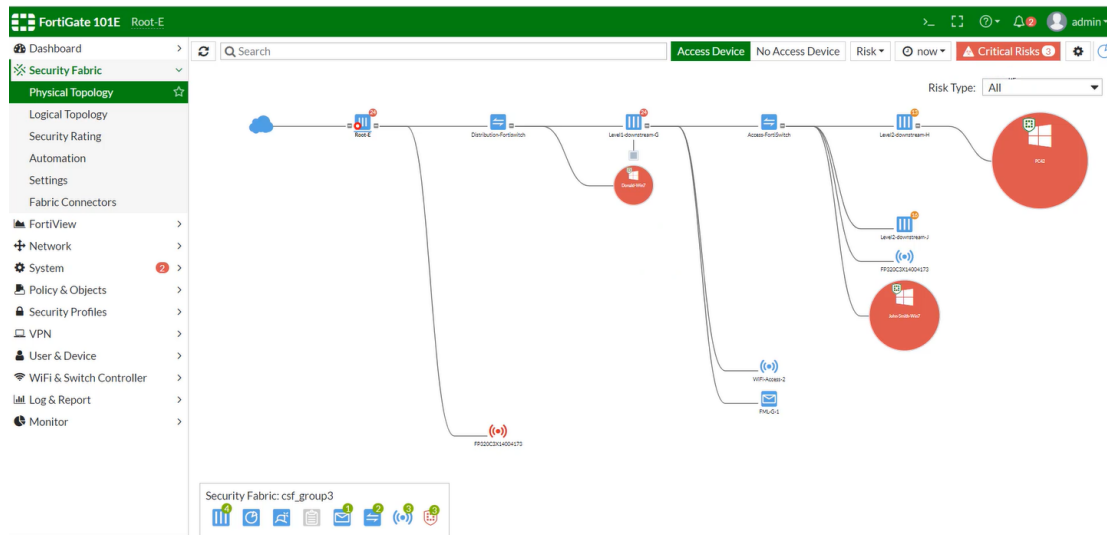
To access the consolidated Risk view mode:

1. In the view option dropdown button, select *Risk*.

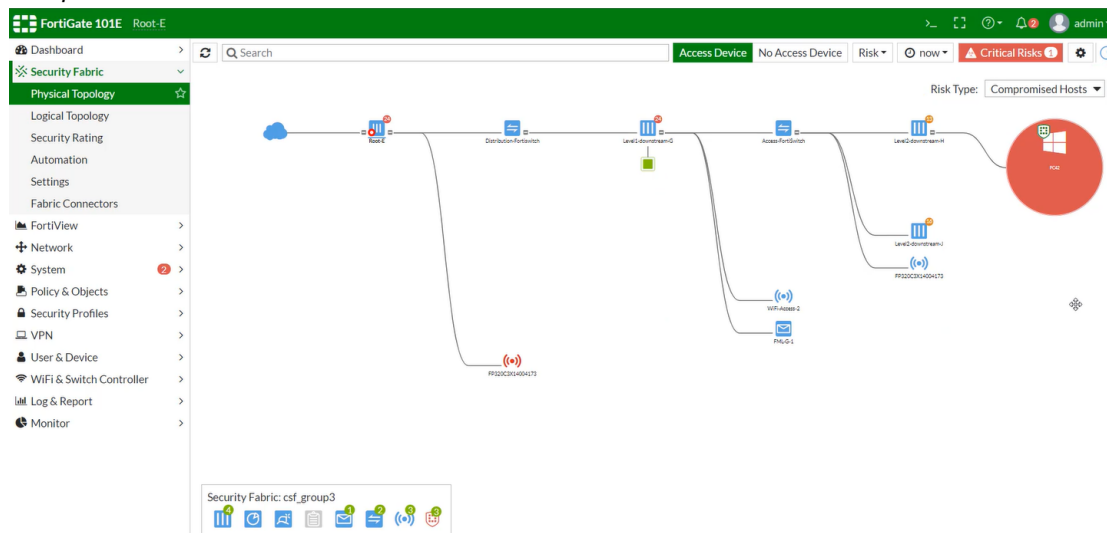


2. Select one of the following options from the *Risk Type* dropdown menu:

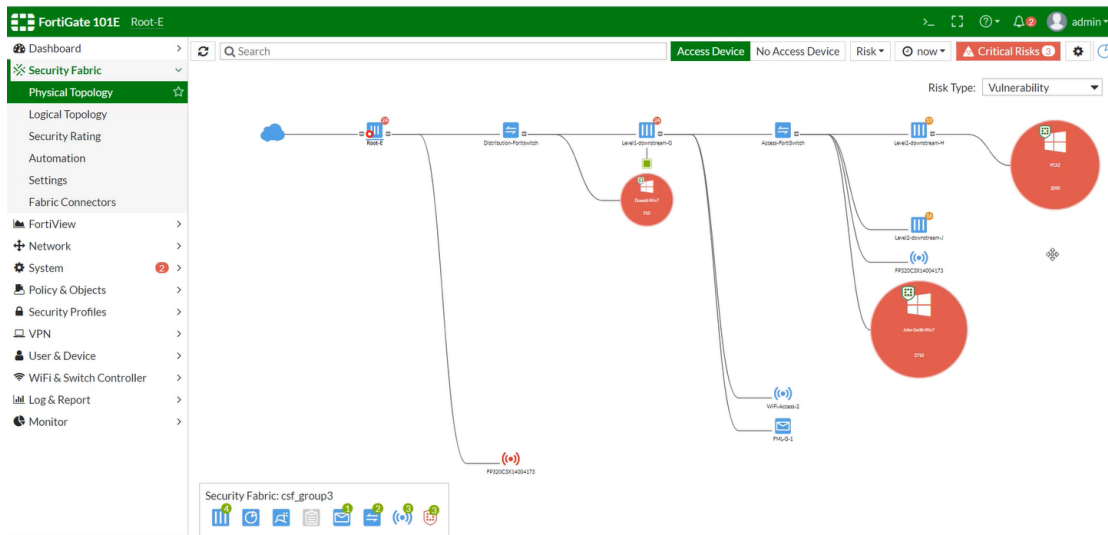
- *All*



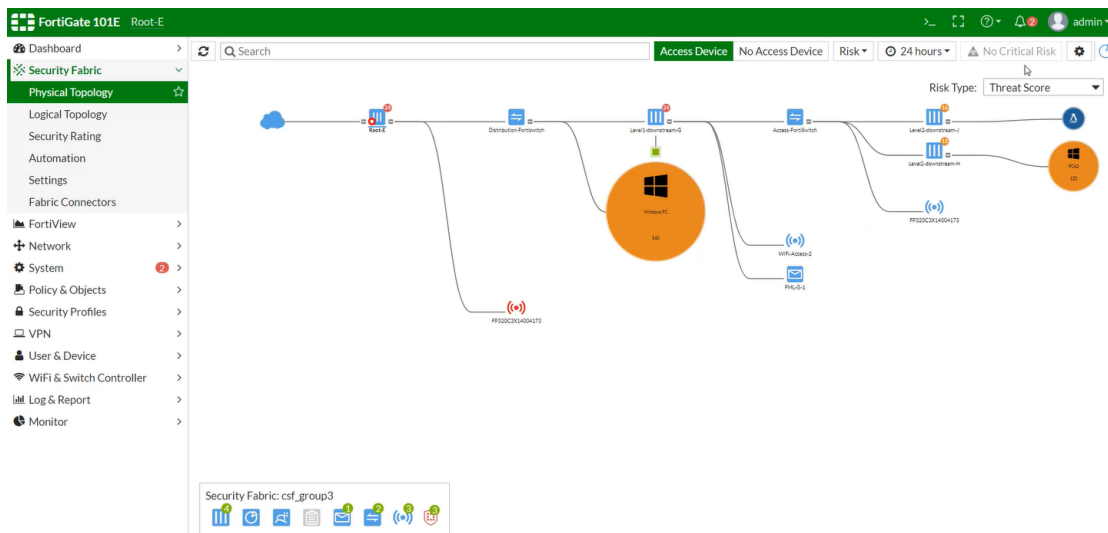
- *Compromised Hosts*



- **Vulnerability**



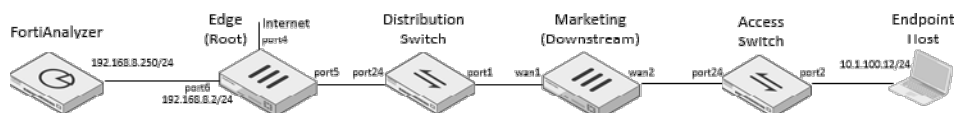
- **Threat Score**



Viewing and controlling network risks via topology view

This example shows how to view and control compromised hosts via the *Security Fabric > Physical Topology* or *Security Fabric > Logical Topology* view.

In the following topology, the downstream FortiGate (Marketing) is connected to the root FortiGate (Edge) through a FortiSwitch (Distribution). The Endpoint Host is connected to the downstream FortiGate (Marketing) through another FortiSwitch (Access).



This example consists of the following steps:

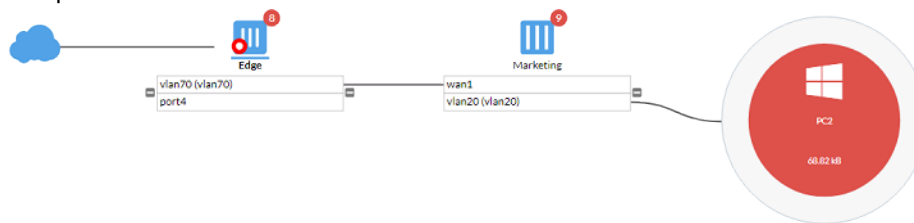
1. View the compromised endpoint host.
2. Quarantine the compromised endpoint host.
3. Run `diagnose` commands.

To view the compromised endpoint host:

1. Test that FortiGate detects a compromised endpoint host by opening a browser on the endpoint host and entering a malicious website URL. The browser displays a *Web Page Blocked!* warning and does not allow access to the website.
2. In FortiOS on the root FortiGate, go to *Security Fabric > Physical Topology*. The endpoint host, connected to the Access FortiSwitch, is highlighted in red. Mouse over the endpoint host to view a tooltip that shows the IOC verdict. The endpoint host is compromised.



3. Go to *Security Fabric > Logical Topology*. The endpoint host, connected to the downstream FortiGate, is highlighted in red. Mouse over the endpoint host to view a tooltip that shows the IOC verdict. The endpoint host is compromised.



To quarantine the compromised endpoint host:

1. In FortiOS on the root FortiGate, go to *Security Fabric > Physical Topology*.
2. Right-click the endpoint host and select *Quarantine Host*. Click *OK* to confirm the confirmation dialog.
3. Go to *Monitor > Quarantine Monitor*. From the dropdown list at the top right corner, select *All FortiGates*. The quarantined endpoint host displays in the content pane.
4. On the endpoint host, open a browser and visit a website such as <https://www.fortinet.com/>. If the website cannot be accessed, this confirms that the endpoint host is quarantined.

To run diagnose commands:

1. To show the downstream FortiGate after it joins the Security Fabric, run the `diagnose sys csf downstream` command in the root FortiGate (Edge) CLI. The output should resemble the following:


```
Edge # diagnose sys csf downstream
1: FG101ETK18000000 (192.168.7.3) Management-IP: 0.0.0.0 Management-port:0 parent:
   FG201ETK18900000
path:FG201ETK18900000:FG101ETK18000000
data received: Y downstream intf:wan1 upstream intf:vlan70 admin-port:443
authorizer:FG201ETK18900000
```
2. To show the upstream FortiGate after the downstream FortiGate joins the Security Fabric, run the `diagnose sys csf upstream` command in the downstream FortiGate (Marketing) CLI. The output should resemble the following:

```
Marketing # diagnose sys csf upstream
```

```
Upstream Information:
Serial Number:FG201ETK18900000
IP:192.168.7.2
Connecting interface:wan1
Connection status:Authorized
```

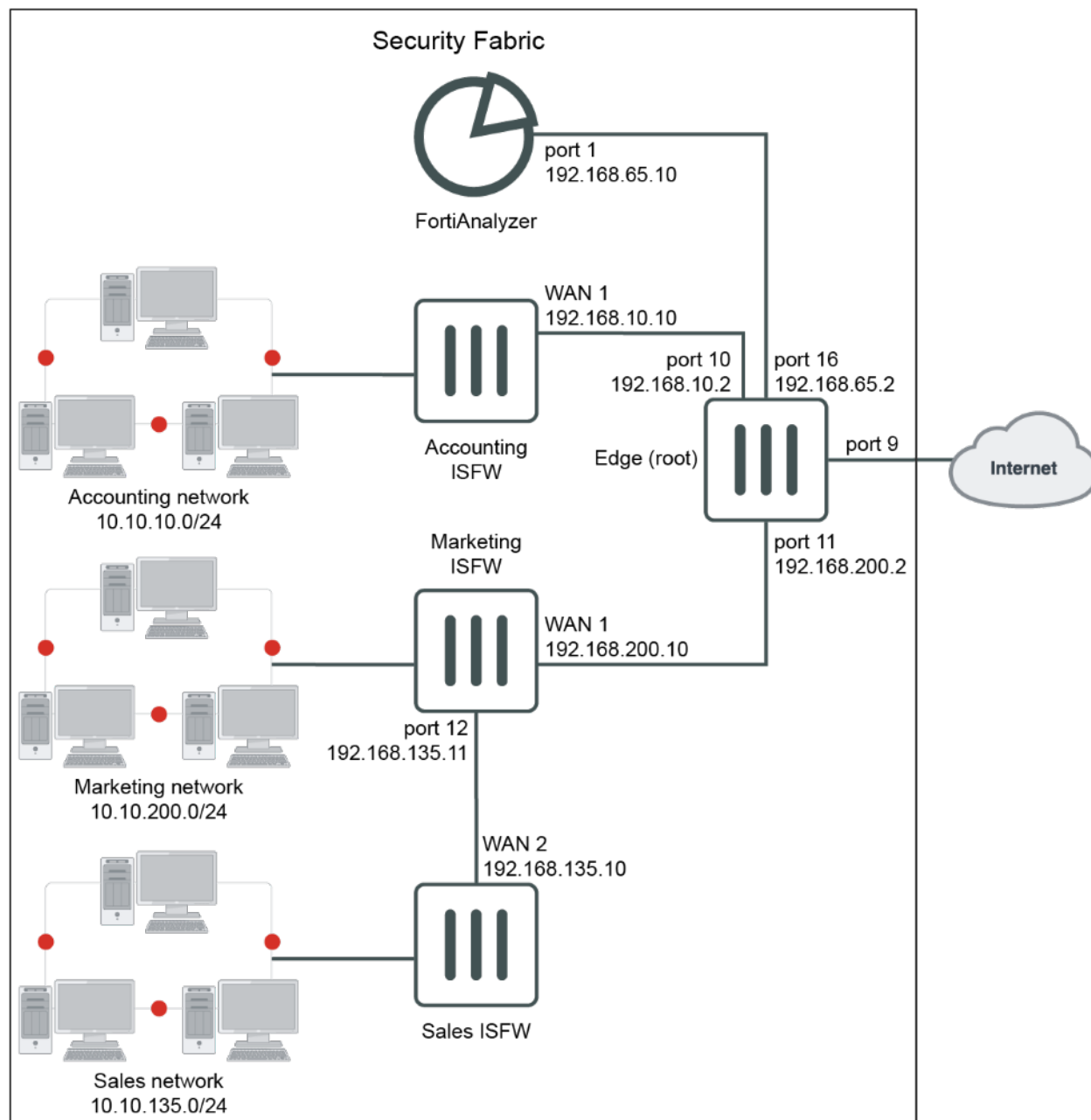
3. To show the quarantined endpoint host in the connected FortiGate, run the following commands in the downstream FortiGate (Marketing) CLI:

```
Marketing # show user quarantine
config user quarantine
  config targets
    edit "PC2"
      set description "Manually quarantined"
      config macs
        edit 00:0c:29:3d:89:39
          set description "manual-qtn Hostname: PC2"
        next
      end
    next
  end
end
```

Deploying the Security Fabric

This topic provides an example of deploying Security Fabric with three downstream FortiGates connecting to one root FortiGate. To deploy Security Fabric, you need a FortiAnalyzer running firmware version 6.2 or later.

The following shows a sample network topology with three downstream FortiGates (Accounting, Marketing, and Sales) connected to the root FortiGate (Edge).



To configure the root FortiGate (Edge):

1. Configure interfaces:
 - a. In the root FortiGate (Edge), go to *Network > Interfaces*.
 - b. Edit *port16*:
 - Set *Role* to *DMZ*.
 - For the interface connected to FortiAnalyzer, set the *IP/Network Mask* to *192.168.65.2/255.255.255.0*

- c. Edit *port10*:
 - Set *Role* to *LAN*.
 - For the interface connected to the downstream FortiGate (Accounting), set the *IP/Network Mask* to *192.168.10.2/255.255.255.0*
- d. Edit *port11*:
 - Set *Role* to *LAN*.
 - For the interface connected to the downstream FortiGate (Marketing), set the *IP/Network Mask* to *192.168.200.2/255.255.255.0*
2. Configure Security Fabric:
 - a. In the root FortiGate (Edge), go to *Security Fabric > Settings*.
 - b. Enable *FortiGate Telemetry*.
After *FortiGate Telemetry* is enabled, FortiAnalyzer automatically enables *Logging* and *Upload Option* is set to *Real Time*.
 - c. Set a *Fabric name*, such as *Office-Security-Fabric*.
 - d. Enable *Allow other FortiGates to join* and add *port10* and *port11*.
 - e. Under *FortiAnalyzer Logging*, set *IP address* to the FortiAnalyzer IP *192.168.65.10*.
 - f. Click *Test Connectivity*.
A warning message indicates that the FortiGate is not authorized on the FortiAnalyzer. The authorization is configured in a later step on the FortiAnalyzer.
 - g. Click *Apply*.
3. Create a policy to allow the downstream FortiGate (Accounting) to access the FortiAnalyzer:
 - a. In the root FortiGate (Edge), go to *Policy & Objects > Addresses*.
 - b. Click *Create New*.
 - Set *Name* to *FAZ-addr*.
 - Set *Type* to *Subnet*.
 - Set *Subnet/IP Range* to *192.168.65.10/32*.
 - Set *Interface* to *any*.
 - c. Click *OK*.
 - d. Click *Create New*.
 - Set *Name* to *Accounting*.
 - Set *Type* to *Subnet*.
 - Set *Subnet/IP Range* to *192.168.10.10/32*.
 - Set *Interface* to *any*.
 - e. Click *OK*.
 - f. In the root FortiGate (Edge), go to *Policy & Objects > IPv4 Policy* and click *Create New*.
 - Set *Name* to *Accounting-to-FAZ*.
 - Set *srcintf* to *port10*.
 - Set *dstintf* to *port16*.
 - Set *srcaddr* to *Accounting-addr*.
 - Set *dstaddr* to *FAZ-addr*.
 - Set *Action* to *Accept*.
 - Set *Schedule* to *Always*.
 - Set *Service* to *All*.
 - Enable *NAT*.
 - Set *IP Pool Configuration* to *Use Outgoing Interface Address*.
 - g. Click *OK*.

4. Create a policy to allow the two downstream FortiGates (Marketing and Sales) to access the FortiAnalyzer:

- a. In the root FortiGate (Edge), go to *Policy & Objects > Addresses* and click *Create New*.
 - Set *Name* to *Marketing-addr*.
 - Set *Type* to *Subnet*.
 - Set *Subnet/IP Range* to *192.168.200.10/32*.
 - Set *Interface* to *any*.
- b. Click *OK*.
- c. In the root FortiGate (Edge), go to *Policy & Objects > IPv4 Policy* and click *Create New*.
 - Set *Name* to *Marketing-to-FAZ*.
 - Set *srcintf* to *port11*.
 - Set *dstintf* to *port16*.
 - Set *srcaddr* to *Marketing-addr*.
 - Set *dstaddr* to *FAZ-addr*.
 - Set *Action* to *Accept*.
 - Set *Schedule* to *Always*.
 - Set *Service* to *All*.
 - Enable *NAT*.
 - Set *IP Pool Configuration* to *Use Outgoing Interface Address*.
- d. Click *OK*.

To configure the downstream FortiGate (Accounting):

1. Configure interface:
 - a. In the downstream FortiGate (Accounting), go to *Network > Interfaces*.
 - b. Edit interface *wan1*:
 - Set *Role* to *WAN*.
 - For the interface connected to root, set the *IP/Network Mask* to *192.168.10.10/255.255.255.0*
2. Configure the default static route to connect to the root FortiGate (Edge):
 - a. In the downstream FortiGate (Accounting), go to *Network > Static Routes* and click *Create New* or *Create New > IPv4 Static Route*.
 - Set *Destination* to *0.0.0.0/0.0.0.0*.
 - Set *Interface* to *wan1*.
 - Set *Gateway Address* to *192.168.10.2*.
 - b. Click *OK*.
3. Configure Security Fabric:
 - a. In the downstream FortiGate (Accounting), go to *Security Fabric > Settings*.
 - b. Enable *FortiGate Telemetry*.

After *FortiGate Telemetry* is enabled, FortiAnalyzer automatically enables *Logging*. Settings for the FortiAnalyzer are retrieved from the root FortiGate (Edge) when FortiGate (Accounting) connects to the root FortiGate (Edge).
 - c. Set *Security Fabric role* to *Join Existing Fabric*.
 - d. *Upstream FortiGate IP* is filled in automatically with the default static route *Gateway Address* of *192.168.10.2* set in the previous step.
 - e. Leave *Allow other FortiGates to join* disabled, because there is no downstream FortiGate connecting to it.
 - f. Click *Apply*.

To configure the downstream FortiGate (Marketing):

1. Configure interface:
 - a. In the downstream FortiGate (Marketing), go to *Network > Interfaces*.
 - b. Edit *port12*:
 - Set *Role* to *LAN*.
 - For the interface connected to the downstream FortiGate (Sales), set the *IP/Network Mask* to *192.168.135.11/255.255.255.0*.
 - c. Edit *wan1*:
 - Set *Role* to *WAN*.
 - For the interface connected to the root FortiGate (Edge), set the *IP/Network Mask* to *192.168.200.10/255.255.255.0*.
2. Configure the default static route to connect to the root FortiGate (Edge):
 - a. In the downstream FortiGate (Marketing), go to *Network > Static Routes* and click *Create New* or *Create New > IPv4 Static Route*.
 - Set *Destination* to *0.0.0.0/0.0.0.0*.
 - Set *Interface* to *wan1*.
 - Set *Gateway Address* to *192.168.200.2*.
 - b. Click *OK*.
3. Configure Security Fabric:
 - a. In the downstream FortiGate (Marketing), go to *Security Fabric > Settings*.
 - b. Enable *FortiGate Telemetry*.

After *FortiGate Telemetry* is enabled, FortiAnalyzer automatically enables *Logging*. Settings for the FortiAnalyzer are retrieved from the root FortiGate (Edge) when FortiGate (Marketing) connects to the root FortiGate (Edge).
 - c. Set *Security Fabric role* to *Join Existing Fabric*.
 - d. *Upstream FortiGate IP* is filled in automatically with the default static route *Gateway Address* of *192.168.200.2* set in the previous step.
 - e. Enable *Allow other FortiGates to join* and add *port12*.
 - f. Click *Apply*.
4. Create a policy to allow another downstream FortiGate (Sales) going through FortiGate (Marketing) to access the FortiAnalyzer:
 - a. In the downstream FortiGate (Marketing), go to *Policy & Objects > Addresses* and click *Create New*.
 - Set *Name* to *FAZ-addr*.
 - Set *Type* to *Subnet*.
 - Set *Subnet/IP Range* to *192.168.65.10/32*.
 - Set *Interface* to *any*.
 - b. Click *OK*.
 - c. Click *Create New*.
 - Set *Name* to *Sales-addr*.
 - Set *Type* to *Subnet*.
 - Set *Subnet/IP Range* to *192.168.135.10/32*.
 - Set *Interface* to *any*.
 - d. Click *OK*.

- e. In the downstream FortiGate (Marketing), go to *Policy & Objects > IPv4 Policy* and click *Create New*.
 - Set *Name* to *Sales-to-FAZ*.
 - Set *srcintf* to *port12*.
 - Set *dstintf* to *wan1*.
 - Set *srcaddr* to *Sales-addr*.
 - Set *dstaddr* to *FAZ-addr*.
 - Set *Action* to *Accept*.
 - Set *Schedule* to *Always*.
 - Set *Service* to *All*.
 - Enable *NAT*.
 - Set *IP Pool Configuration* to *Use Outgoing Interface Address*.
- f. Click *OK*.

To configure the downstream FortiGate (Accounting):

1. Configure interface:
 - a. In the downstream FortiGate (Accounting), go to *Network > Interfaces*.
 - b. Edit interface *wan1*:
 - Set *Role* to *WAN*.
 - For the interface connected to root, set the *IP/Network Mask* to *192.168.10.10/255.255.255.0*
2. Configure the default static route to connect to the root FortiGate (Edge):
 - a. In the downstream FortiGate (Accounting), go to *Network > Static Routes* and click *Create New* or *Create New > IPv4 Static Route*.
 - Set *Destination* to *0.0.0.0/0.0.0.0*.
 - Set *Interface* to *wan1*.
 - Set *Gateway Address* to *192.168.10.2*.
 - b. Click *OK*.
3. Configure Security Fabric:
 - a. In the downstream FortiGate (Accounting), go to *Security Fabric > Settings*.
 - b. Enable *FortiGate Telemetry*.

After *FortiGate Telemetry* is enabled, FortiAnalyzer automatically enables *Logging*. Settings for the FortiAnalyzer are retrieved from the root FortiGate (Edge) when FortiGate (Accounting) connects to the root FortiGate (Edge).
 - c. Set *Security Fabric role* to *Join Existing Fabric*.
 - d. *Upstream FortiGate IP* is filled in automatically with the default static route *Gateway Address* of *192.168.10.2* set in the previous step.
 - e. Leave *Allow other FortiGates to join* disabled, because there is no downstream FortiGate connecting to it.
 - f. Click *Apply*.

To configure the downstream FortiGate (Sales):

1. Configure interface:
 - a. In the downstream FortiGate (Sales), go to *Network > Interfaces*.
 - b. Edit *wan2*:
 - Set *Role* to *WAN*.
 - For the interface connected to the upstream FortiGate (Marketing), set the *IP/Network Mask* to *192.168.135.10/255.255.255.0*.

2. Configure the default static route to connect to the upstream FortiGate (Marketing):
 - a. In the downstream FortiGate (Sales), go to *Network > Static Routes* and click *Create New* or *Create New > IPv4 Static Route*.
 - Set *Destination* to *0.0.0.0/0.0.0.0*.
 - Set *Interface* to *wan2*.
 - Set *Gateway Address* to *192.168.135.11*.
 - b. Click *OK*.
3. Configure Security Fabric:
 - a. In the downstream FortiGate (Sales), go to *Security Fabric > Settings*.
 - b. Enable *FortiGate Telemetry*.

After *FortiGate Telemetry* is enabled, FortiAnalyzer automatically enables *Logging*. Settings for the FortiAnalyzer are retrieved from the root FortiGate (Edge) when FortiGate (Sales) connects to the root FortiGate (Edge).
 - c. Set *Security Fabric* role to *Join Existing Fabric*.
 - d. *Upstream FortiGate IP* is filled in automatically with the default static route *Gateway Address* of *192.168.135.11* set in the previous step.
 - e. Leave *Allow other FortiGates to join* disabled, because there is no downstream FortiGate connecting to it.
 - f. Click *Apply*.

To authorize downstream FortiGates (Accounting, Marketing, and Sales) on the root FortiGate (Edge):

1. In the root FortiGate (Edge), go to *Security Fabric > Settings*.

The *Topology* field highlights two connected FortiGates with their serial numbers and asks you to authorize the highlighted devices.
2. Select the highlighted FortiGates and select *Authorize*.

After they are authorized, the two downstream FortiGates (Accounting and Marketing) appear in the *Topology* field in *Security Fabric > Settings*. This means that the two downstream FortiGates (Accounting and Marketing) have successfully joined the Security Fabric.
3. The *Topology* field now highlights the FortiGate with the serial number that is connected to the downstream FortiGate (Marketing) and asks you to authorize the highlighted device.
4. Select the highlighted FortiGates and select *Authorize*.

After it is authorized, the downstream FortiGate (Sales) appears in the *Topology* field in *Security Fabric > Settings*. This means that the downstream FortiGates (Sales) has successfully joined the Security Fabric.

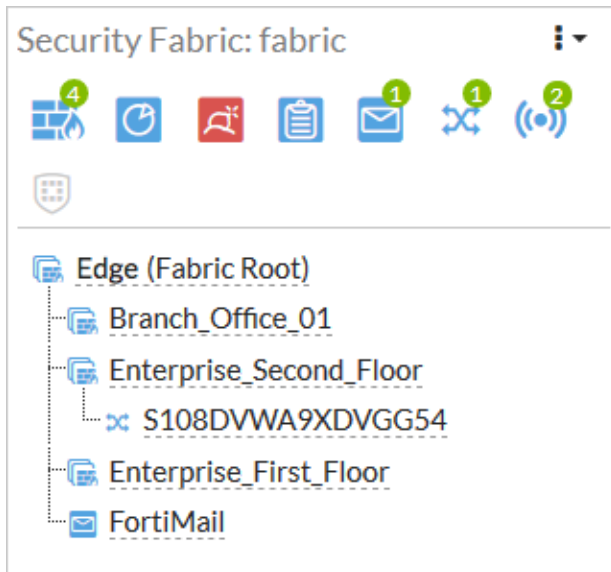
To use FortiAnalyzer to authorize all the Security Fabric FortiGates:

1. Authorize all the Security Fabric FortiGates on the FortiAnalyzer side:
 - a. On the FortiAnalyzer, go to *System Settings > Network > All Interfaces*.
 - b. Edit *port1* and set *IP Address/Netmask* to *192.168.65.10/255.255.255.0*.
 - c. Go to *Device Manager > Unauthorized*. All of the FortiGates are listed as unauthorized.
 - i. Select all the FortiGates and select *Authorize*. The FortiGates are now listed as authorized.

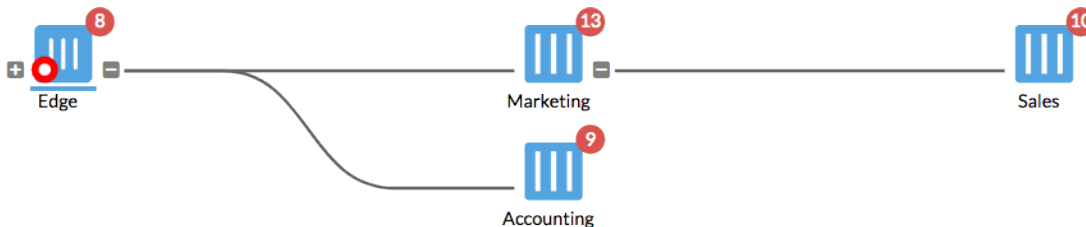
After a moment, a warning icon appears beside the root FortiGate (Edge) because the FortiAnalyzer needs administrative access to the root FortiGate (Edge) in the Security Fabric.
 - ii. Click the warning icon and enter the admin username and password of the root FortiGate (Edge).
2. Check FortiAnalyzer status on all the Security Fabric FortiGates:
 - a. On each FortiGates, go to *Security Fabric > Settings* and check that *FortiAnalyzer Logging* shows *Storage usage* information.

To check Security Fabric deployment result:

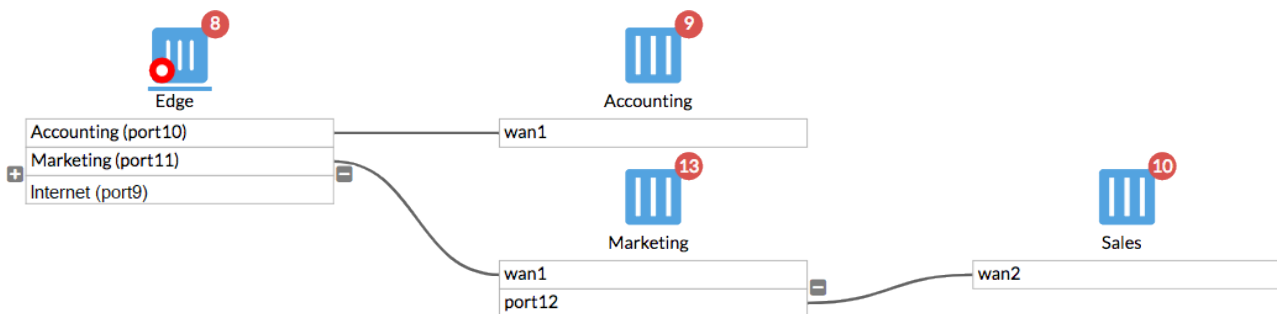
1. On FortiGate (Edge), go to *Dashboard > Status*.
The *Security Fabric* widget displays all the FortiGates in the Security Fabric.



2. On FortiGate (Edge), go to *Security Fabric > Physical Topology*.
This page shows a visualization of access layer devices in the Security Fabric.



3. On FortiGate (Edge), go to *Security Fabric > Physical Topology*.
This dashboard shows information about the interfaces of each device in the Security Fabric.

**To run diagnose commands:**

1. Run the `diagnose sys csf authorization pending-list` command in the root FortiGate to show the downstream FortiGate pending for root FortiGate authorization:

```
Edge # diagnose sys csf authorization pending-list
Serial          IP Address      HA-Members      Path
```

```
-----
FG201ETK18902514          0.0.0.0          FG3H1E5818900718:FG201ETK18902514
```

2. Run the `diagnose sys csf downstream` command in the root or middle FortiGate to show the downstream FortiGates after they join Security Fabric:

```
Edge # diagnose sys csf downstream
1:      FG201ETK18902514 (192.168.200.10) Management-IP: 0.0.0.0 Management-port:0
parent: FG3H1E5818900718
        path:FG3H1E5818900718:FG201ETK18902514
        data received: Y downstream intf:wan1 upstream intf:port11 admin-port:443
        authorizer:FG3H1E5818900718
2:      FGT81ETK18002246 (192.168.10.10) Management-IP: 0.0.0.0 Management-port:0 parent:
FG3H1E5818900718
        path:FG3H1E5818900718:FGT81ETK18002246
        data received: Y downstream intf:wan1 upstream intf:port10 admin-port:443
        authorizer:FG3H1E5818900718
3:      FG101ETK18002187 (192.168.135.10) Management-IP: 0.0.0.0 Management-port:0
parent: FG201ETK18902514
        path:FG3H1E5818900718:FG201ETK18902514:FG101ETK18002187
        data received: Y downstream intf:wan2 upstream intf:port12 admin-port:443
        authorizer:FG3H1E5818900718
```

3. Run the `diagnose sys csf upstream` command in any downstream FortiGate to show the upstream FortiGate after downstream FortiGate joins Security Fabric:

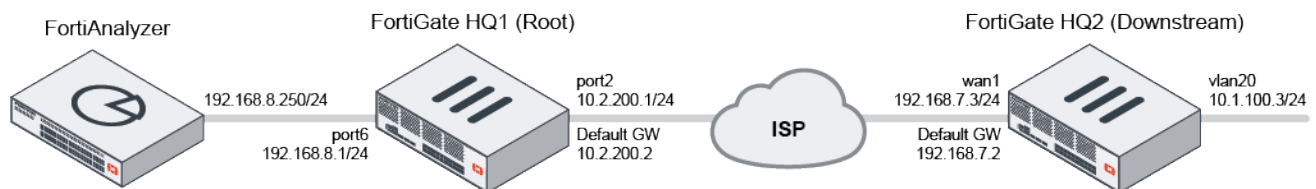
```
Marketing # diagnose sys csf upstream
Upstream Information:
Serial Number:FG3H1E5818900718
IP:192.168.200.2
Connecting interface:wan1
Connection status:Authorized
```

Security Fabric over IPsec VPN

This is an example of configuring Security Fabric over IPsec VPN.

Sample topology

This sample topology shows a downstream FortiGate (HQ2) connected to the root FortiGate (HQ1) over IPsec VPN to join Security Fabric.



Sample configuration

To configure the root FortiGate (HQ1):

1. Configure interface:
 - a. In the root FortiGate (HQ1), go to *Network > Interfaces*.
 - b. Edit *port2*:
 - Set *Role* to *WAN*.
 - For the interface connected to the Internet, set the *IP/Network Mask* to *10.2.200.1/255.255.255.0*
 - c. Edit *port6*:
 - Set *Role* to *DMZ*.
 - For the interface connected to FortiAnalyzer, set the *IP/Network Mask* to *192.168.8.250/255.255.255.0*
2. Configure the static route to connect to the Internet:
 - a. Go to *Network > Static Routes* and click *Create New* or *Create New > IPv4 Static Route*.
 - Set *Destination* to *0.0.0.0/0.0.0.0*.
 - Set *Interface* to *port2*.
 - Set *Gateway Address* to *10.2.200.2*.
 - b. Click *OK*.
3. Configure IPsec VPN:
 - a. Go to *VPN > IPsec Wizard*.
 - Set *Name* to *To-HQ2*.
 - Set *Template Type* to *Custom*.
 - Click *Next*.
 - Set *Authentication* to *Method*.
 - Set *Pre-shared Key* to *123456*.
 - b. Leave all other fields in their default values and click *OK*.
4. Configure the IPsec VPN interface IP address which will be used to form Security Fabric:
 - a. Go to *Network > Interfaces*.
 - b. Edit *To-HQ2*:
 - Set *Role* to *LAN*.
 - Set the *IP/Network Mask* to *10.10.10.1/255.255.255.255*.
 - Set *Remote IP/Network Mask* to *10.10.10.3/255.255.255.0*.
5. Configure IPsec VPN local and remote subnet:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Click *Create New*
 - Set *Name* to *To-HQ2_remote_subnet_2*.
 - Set *Type* to *Subnet*.
 - Set *IP/Network Mask* to *10.10.10.3/32*.
 - c. Click *OK*.
 - d. Click *Create New*
 - Set *Name* to *To-HQ2_local_subnet_1*.
 - Set *Type* to *Subnet*.
 - Set *IP/Network Mask* to *192.168.8.0/24*.
 - e. Click *OK*.

- f. Click *Create New*
 - Set *Name* to *To-HQ2_remote_subnet_1*.
 - Set *Type* to *Subnet*.
 - Set *IP/Network Mask* to *10.1.100.0/24*.
 - g. Click *OK*.
 6. Configure IPsec VPN static routes:
 - a. Go to *Network > Static Routes*
 - b. Click *Create New* or *Create New > IPv4 Static Route*.
 - For *Named Address*, select *Type* and select *To-HQ2_remote_subnet_1*.
 - Set *Interface* to *To-HQ2*.Click *OK*.
 - c. Click *Create New* or *Create New > IPv4 Static Route*.
 - For *Named Address*, select *Type* and select *To-HQ2_remote_subnet_1*.
 - Set *Interface* to *Blackhole*.
 - Set *Administrative Distance* to *254*.
 - d. Click *OK*.
 7. Configure IPsec VPN policies:
 - a. Go to *Policy & Objects > IPv4 Policy*
 - b. Click *Create New*.
 - Set *Name* to *vpn_To-HQ2_local*.
 - Set *Incoming Interface* to *port6*.
 - Set *Outgoing Interface* to *To-HQ2*.
 - Set *Source* to *To-HQ2_local_subnet_1*.
 - Set *Destination* to *To-HQ2_remote_subnet_1*.
 - Set *Schedule* to *Always*.
 - Set *Service* to *All*.
 - Disable *NAT*.
 - c. Click *OK*.
 - d. Click *Create New*.
 - Set *Name* to *vpn_To-HQ2_remote*.
 - Set *Incoming Interface* to *To-HQ2*.
 - Set *Outgoing Interface* to *port6*.
 - Set *Source* to *To-HQ2_remote_subnet_1, To-HQ2_remote_subnet_2*.
 - Set *Destination* to *To-HQ2_local_subnet_1*.
 - Set *Schedule* to *Always*.
 - Set *Service* to *All*.
 - Enable *NAT*.
 - Set *IP Pool Configuration* to *Use Outgoing Interface Address*.
 - e. Click *OK*.
 8. Configure Security Fabric:
 - a. Go to *Security Fabric > Settings*.
 - b. Enable *FortiGate Telemetry*.

After *FortiGate Telemetry* is enabled, FortiAnalyzer automatically enables *Logging* and *Upload* is set to *Real Time*.
 - c. Set *Fabric name* to *Office-Security-Fabric*.

- d. Enable *Allow other FortiGates to join* and add VPN interface *To-HQ2*.
- e. Under *FortiAnalyzer Logging*, set *IP address* to the FortiAnalyzer IP of 192.168.8.250.
- f. Click *Apply*.

To configure the downstream FortiGate (HQ2):

1. Configure interface:
 - a. Go to *Network > Interfaces*.
 - b. Edit interface *wan1*:
 - Set *Role* to *WAN*.
 - For the interface connected to the Internet, set the *IP/Network Mask* to 192.168.7.3/255.255.255.0.
 - c. Edit interface *vlan20*:
 - Set *Role* to *LAN*.
 - For the interface connected to local endpoint clients, set the *IP/Network Mask* to 10.1.100.3/255.255.255.0.
2. Configure the static route to connect to the Internet:
 - a. Go to *Network > Static Routes* and click *Create New* or *Create New > IPv4 Static Route*.
 - Set *Destination* to 0.0.0.0/0.0.0.0.
 - Set *Interface* to *wan1*.
 - Set *Gateway Address* to 192.168.7.2.
 - b. Click *OK*.
3. Configure IPsec VPN:
 - a. Go to *VPN > IPsec Wizard*.
 - Set *VPN Name* to *To-HQ1*.
 - Set *Template Type* to *Custom*.
 - Click *Next*.
 - In the *Network IP Address*, enter 10.2.200.1.
 - Set *Interface* to *wan1*.
 - Set *Authentication* to *Method*.
 - Set *Pre-shared Key* to 123456.
 - b. Leave all other fields in their default values and click *OK*.
4. Configure the IPsec VPN interface IP address which will be used to form Security Fabric:
 - a. Go to *Network > Interfaces*.
 - b. Edit *To-HQ1*:
 - Set *Role* to *WAN*.
 - Set the *IP/Network Mask* to 10.10.10.3/255.255.255.255.
 - Set *Remote IP/Network Mask* to 10.10.10.1/255.255.255.0.0.
5. Configure IPsec VPN local and remote subnet:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Click *Create New*
 - Set *Name* to *To-HQ1_local_subnet_1*.
 - Set *Type* to *Subnet*.
 - Set *IP/Network Mask* to 10.1.100.0/24.
 - c. Click *OK*.

- d. Click *Create New*
 - Set *Name* to *To-HQ1_remote_subnet_1*.
 - Set *Type* to *Subnet*.
 - Set *IP/Network Mask* to *192.168.8.0/24*.
 - e. Click *OK*.
 6. Configure IPsec VPN static routes:
 - a. Go to *Network > Static Routes* and click *Create New* or *Create New > IPv4 Static Route*.
 - For *Named Address*, select *Type* and select *To-HQ1_remote_subnet_1*.
 - Set *Interface* to *To-HQ1*.
 - b. Click *OK*.
 - c. Click *Create New* or *Create New > IPv4 Static Route*.
 - For *Named Address*, select *Type* and select *To-HQ1_remote_subnet_1*.
 - Set *Interface* to *Blackhole*.
 - Set *Administrative Distance* to *254*.
 - d. Click *OK*.
 7. Configure IPsec VPN policies:
 - a. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
 - Set *Name* to *vpn_To-HQ1_local*.
 - Set *Incoming Interface* to *vlan20*.
 - Set *Outgoing Interface* to *To-HQ1*.
 - Set *Source* to *To-HQ1_local_subnet_1*.
 - Set *Destination* to *To-HQ1_remote_subnet_1*.
 - Set *Schedule* to *Always*.
 - Set *Service* to *All*.
 - Disable *NAT*.
 - b. Click *OK*.
 - c. Click *Create New*.
 - Set *Name* to *vpn_To-HQ1_remote*.
 - Set *Incoming Interface* to *To-HQ1*.
 - Set *Outgoing Interface* to *vlan20*.
 - Set *Source* to *To-HQ1_remote_subnet_1*.
 - Set *Destination* to *-HQ1_local_subnet_1*.
 - Set *Schedule* to *Always*.
 - Set *Service* to *All*.
 - Disable *NAT*.
 - d. Click *OK*.
 8. Configure Security Fabric:
 - a. Go to *Security Fabric > Settings*.
 - b. Enable *FortiGate Telemetry*.

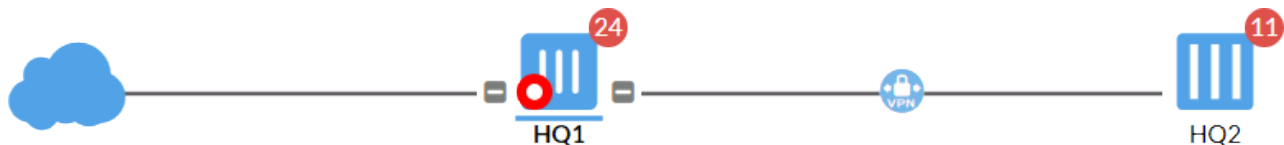
After *FortiGate Telemetry* is enabled, FortiAnalyzer automatically enables *Logging*. FortiAnalyzer settings will be retrieved when the downstream FortiGate connects to the root FortiGate.
 - c. Set *Security Fabric* role to *Join Existing Fabric*.
 - d. Set *Upstream FortiGate IP* to *10.10.10.1*.
 - e. Click *Apply*.

To authorize the downstream FortiGate (HQ2) on the root FortiGate (HQ1):

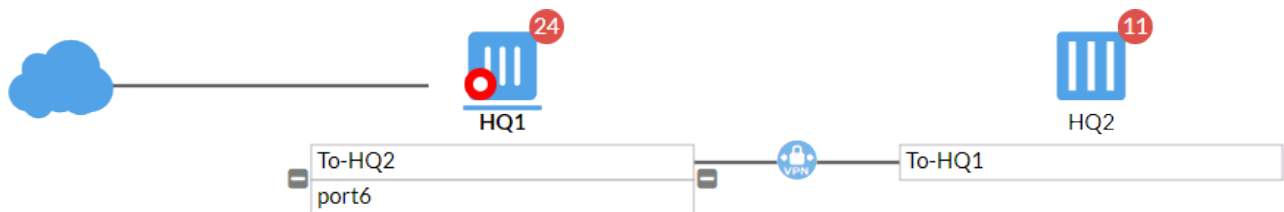
1. In the root FortiGate (HQ1), go to *Security Fabric > Settings*.
The *Topology* field highlights the connected FortiGate (HQ2) with the serial number and asks you to authorize the highlighted device.
2. Select the highlighted FortiGate and select *Authorize*.
After authorization, the downstream FortiGate (HQ2) appears in the *Topology* field in *Security Fabric > Settings*.
This means the downstream FortiGate (HQ2) has successfully joined the Security Fabric.

To check Security Fabric over IPsec VPN:

1. On the root FortiGate (HQ1), go to *Security Fabric > Physical Topology*.
The root FortiGate (HQ1) is connected by the downstream FortiGate (HQ2) with VPN icon in the middle.



2. On the root FortiGate (HQ1), go to *Security Fabric > Logical Topology*.
The root FortiGate (HQ1) VPN interface *To-HQ2* is connected by downstream FortiGate (HQ2) VPN interface *To-HQ1* with VPN icon in the middle.

**To run diagnose commands:**

1. Run the `diagnose sys csf authorization pending-list` command in the root FortiGate (HQ1) to show the downstream FortiGate pending for root FortiGate authorization:

```
HQ1 # diagnose sys csf authorization pending-list
Serial          IP Address      HA-Members
Path
-----
```

```
FG101ETK18002187      0.0.0.0
FG3H1E5818900718:FG101ETK18002187
```

2. Run the `diagnose sys csf downstream` command in the root FortiGate (HQ1) to show the downstream FortiGate (HQ2) after it joins Security Fabric:

```
HQ1 # diagnose sys csf downstream
1:      FG101ETK18002187 (10.10.10.3) Management-IP: 0.0.0.0 Management-port:0 parent:
FG3H1E5818900718
      path:FG3H1E5818900718:FG101ETK18002187
      data received: Y downstream intf:To-HQ1 upstream intf:To-HQ2 admin-port:443
      authorizer:FG3H1E5818900718
```

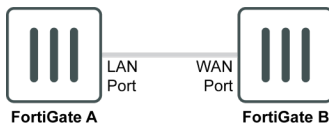
3. Run the `diagnose sys csf upstream` command in the downstream FortiGate (HQ2) to show the root FortiGate (HQ1) after the downstream FortiGate joins Security Fabric:

```
HQ2 # diagnose sys csf upstream
Upstream Information:
Serial Number:FG3H1E5818900718
IP:10.10.10.1
Connecting interface:To-HQ1
Connection status:Authorized
```

Leveraging LLDP to simplify Security Fabric negotiation

This feature enables LLDP reception on WAN interfaces, and prompts FortiGates that are joining the Security Fabric if the upstream FortiGate asks.

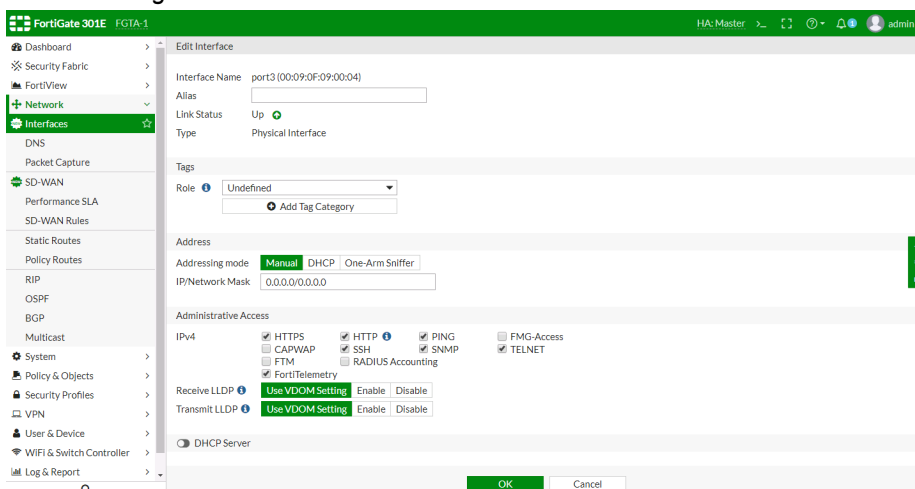
- If an interface's role is undefined, LLDP reception and transmission inherit settings from the VDOM.
- If an interface's role is WAN, LLDP reception is enabled.
- If an interface's role is LAN, LLDP transmission is enabled.



When FortiGate B's WAN interface detects that FortiGate A's LAN interface is immediately upstream (through the default gateway), and FortiGate A has Security Fabric enabled, FortiGate B will show a notification on the GUI asking to join the Security Fabric.

To configure LLDP reception and join a Security Fabric:

1. Go To **Network > Interfaces**.
2. Configure an interface:
 - If the interface's role is undefined, under **Administrative Access**, set **Receive LLDP** and **Transmit LLDP** to **Use VDOM Setting**.



Using the CLI:

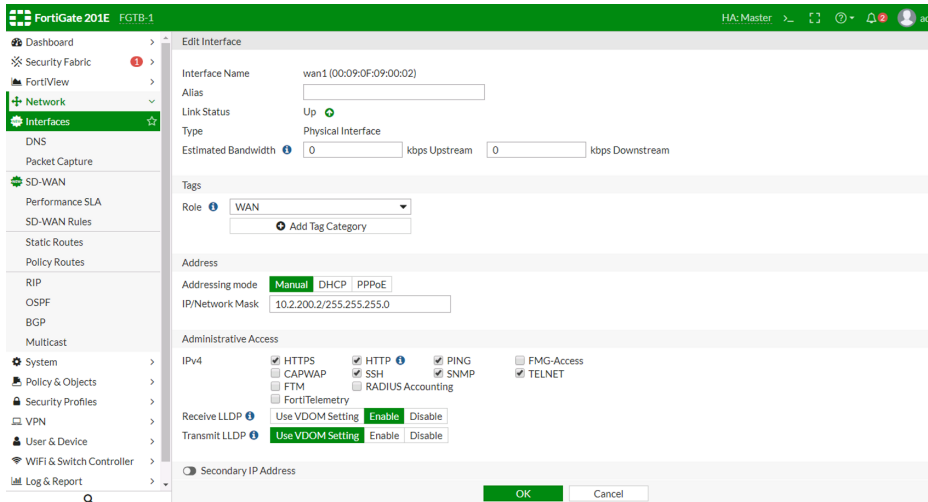
```
config system interface
edit "port3"
set lldp-reception vdom
set lldp-transmission vdom
```

```

set role undefined
...
next
end

```

- If the interface's role is WAN, under *Administrative Access*, set *Receive LLDP* to *Enable* and *Transmit LLDP* to *Use VDOM Setting*.



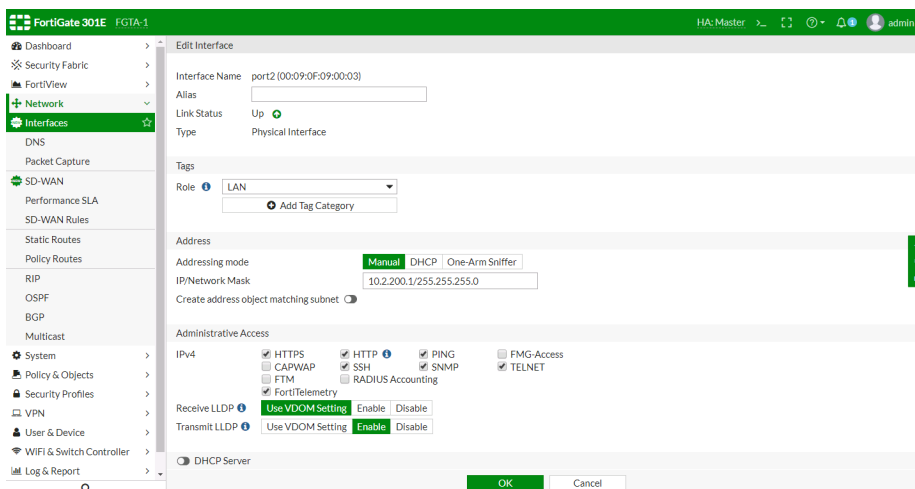
Using the CLI:

```

config system interface
edit "wan1"
set lldp-reception enable
set lldp-transmission vdom
set role wan
...
next
end

```

- If the interface's role is LAN, under *Administrative Access*, set *Receive LLDP* to *Use VDOM Setting* and *Transmit LLDP* to *Enable*.



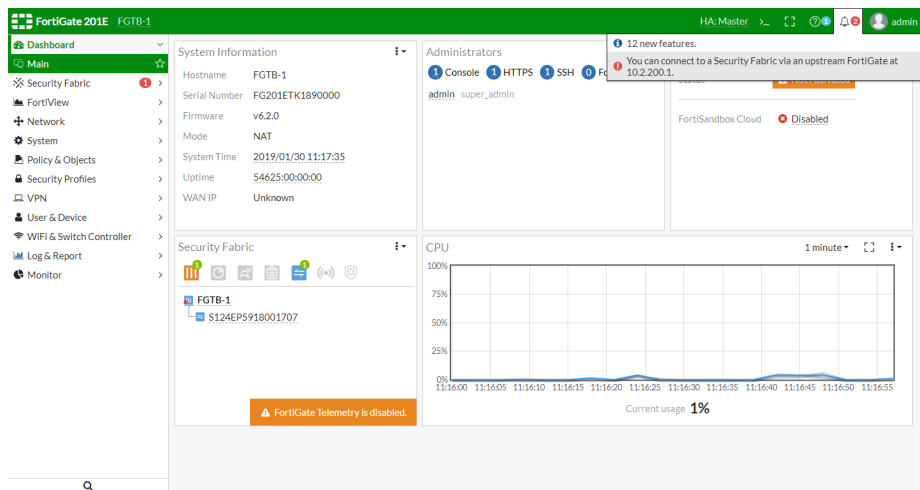
Using the CLI:

```

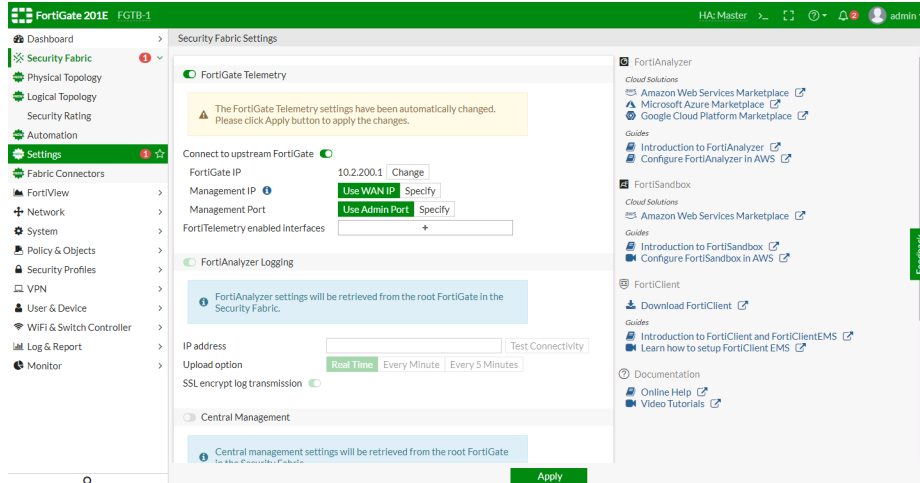
config system interface
  edit "port2"
    set lldp-reception vdom
    set lldp-transmission enable
    set role lan
    ...
  next
end

```

A notification will be shown on FortiGate B.



- Click the notification. The *Security Fabric Settings* page opens with all the required settings automatically configured.



- Click *Apply* to apply the settings, or use the following CLI commands:

```

config system csf
  set status enable
  set upstream-ip 10.2.200.1
end

```

Configuring the Security Fabric with SAML

Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between one Identity Provider (IdP) and one or more Service Providers (SP). Both parties exchange messages using the XML protocol as transport. FortiGate firewall devices can be configured as IdPs or SPs.

When the Security Fabric is enabled, you can configure the root FortiGate as the IdP. You can also configure downstream FortiGates to be automatically configured as SPs, with all links required for SAML communication, when added to the Security Fabric. Administrators must still be authorized on each device. Credentials are verified by the root FortiGate, and login credentials are shared between devices. Once authorized, an administrator can move between fabric devices without logging in again.

Optionally, the downstream FortiGate can also be manually configured as an SP, and then linked to the root FortiGate.

The authentication service is provided by the root FortiGate using local system admin accounts for authentication. Any of the administrator account types can be used for SAML log in. After successful authentication, the administrator logs in to the first downstream FortiGate SP, and can then connect to other downstream FortiGates that have the SSO account properly configured, without needing to provide credentials again, as long as admins use the same browser session. In summary, the root FortiGate IdP performs SAML SSO authentication, and individual device administrators define authorization on FortiGate SPs by using security profiles.

Configuring single-sign-on in the Security Fabric

SAML SSO enables a single FortiGate device to act as the identity provider (IdP), while other FortiGate devices act as service providers (SP) and redirect logins to the IdP.



Only the root FortiGate can be the identity provider (IdP). The downstream FortiGates can be configured as service providers (SP).

The process is as follows:

1. [Configuring the root FortiGate as the IdP on page 120](#)
2. [Configuring a downstream FortiGate as an SP on page 121](#)
3. [Configuring certificates for SAML SSO on page 123](#)
4. [Verifying the single-sign-on configuration on page 124](#)

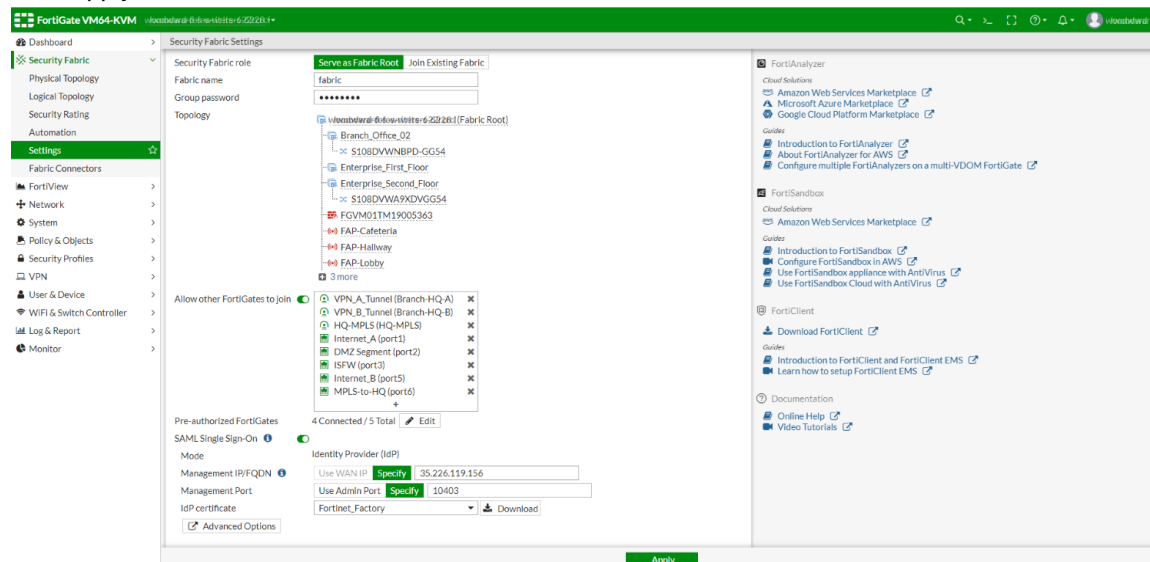
You can also use the CLI. See [CLI commands for SAML SSO on page 125](#).

Configuring the root FortiGate as the IdP

To configure the root FortiGate as the IdP:

1. Log in to the root FortiGate.
2. Go to *Security Fabric > Settings*.
3. In the *FortiGate Telemetry* section, enable *SAML Single Sign-On*. The *Mode* field is automatically populated as *Identity Provider (IdP)*.
4. Enter an IP address in the *Management IP/FQDN* box.

5. Enter a management port in the *Management Port* box.
The *Management IP/FQDN* will be used by the SPs to redirect the login request. The *Management IP/FQDN* and *Management Port* must be reachable from the user's device.
6. Select the *IdP certificate*.
7. Click *Apply*.



Configuring a downstream FortiGate as an SP

There are two ways to configure the downstream FortiGate:

- From the root FortiGate
- From within the downstream device

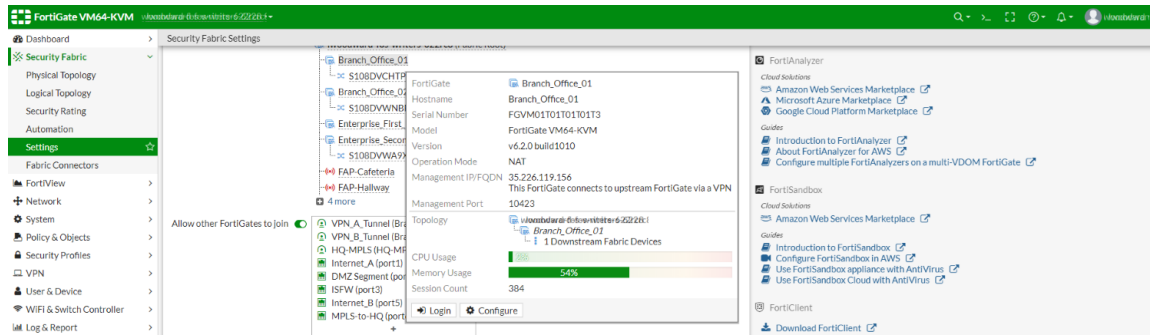


An SP must be a member of the Security Fabric before you configure it.

To configure the downstream FortiGate from the root FortiGate:

1. Log in to the root FortiGate.
2. Go to *Security Fabric > Settings* and locate the *Topology* section.

3. Hover over a FortiGate and click *Configure*.



The *Configure* pane opens.

4. Enable *SAML Single Sign-On*. The *Mode* field is automatically populated as *Service Provider (SP)*.

5. Enter an IP address in the *Management IP/FQDN* box.

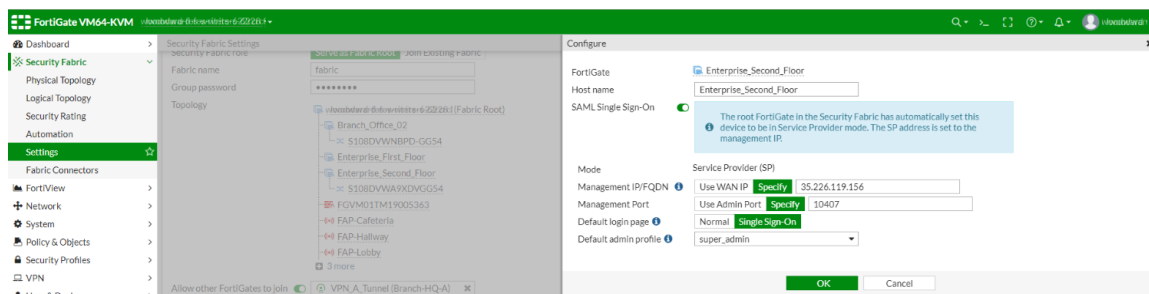
6. Enter a management port in the *Management Port* box.

The *Management IP/FQDN* will be used by the IdP and so other SPs can redirect to each other. The *Management Port* must be reachable from the user's device.

7. Select a *Default login page* option.

8. Select one of the following *Default admin profile* types: *prof_admin*, *super_admin*, or *super_admin_readonly*. The *no_access_admin* profile is set as the default.

9. Click *OK*.



To configure the downstream FortiGate within the device:

1. Log in to the downstream FortiGate.

2. Go to *Security Fabric > Settings*.

3. In the *FortiGate Telemetry* section, enable *SAML Single Sign-On*. The *Mode* field is automatically populated as *Service Provider (SP)*.

4. Enter an IP address in the *Management IP/FQDN* box.

5. Enter a management port in the *Management Port* box.

The *Management IP/FQDN* will be used by the IdP and so other SPs can redirect to each other. The *Management Port* must be reachable from the user's device.

6. Select a *Default login page* option.

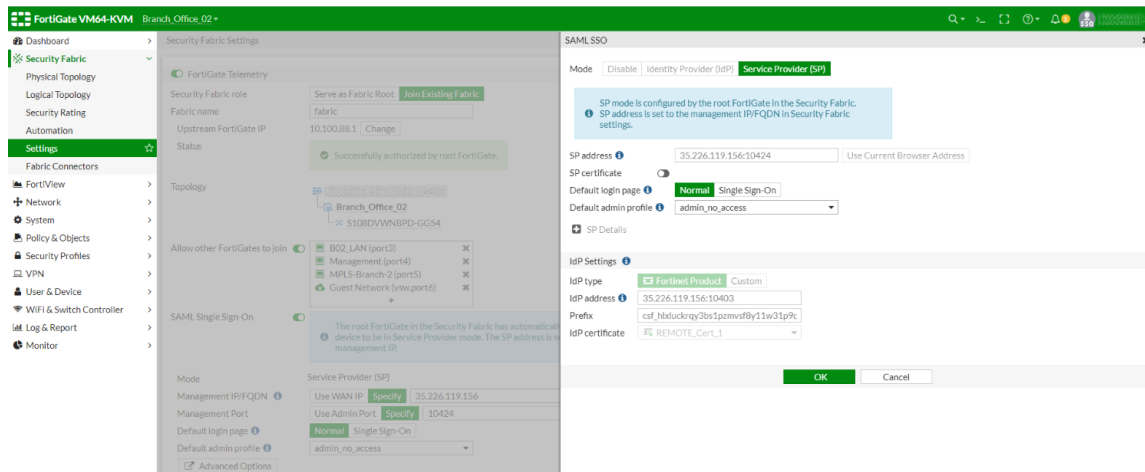
7. Select one of the following *Default admin profile* types: *prof_admin*, *super_admin*, or *super_admin_readonly*. The *no_access_admin* profile is set as the default.

8. Click *OK*.

Configuring certificates for SAML SSO

Because communication between the root FortiGate IdP and FortiGate SPs is secured, you must select a local server certificate in the *IdP certificate* option on the root FortiGate. When downstream SPs join the IdP (root FortiGate), the SP automatically obtains the certificate.

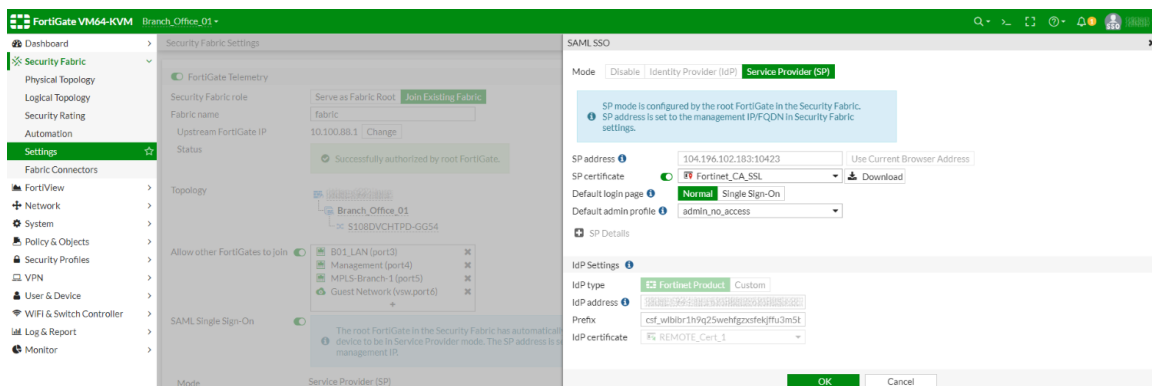
In the following SP example, the *IdP certificate* displays *REMOTE_Cert_1*, which is the root server certificate for the IdP:



It is possible to manually import a certificate from an SP to the IdP so it can be used for authentication.

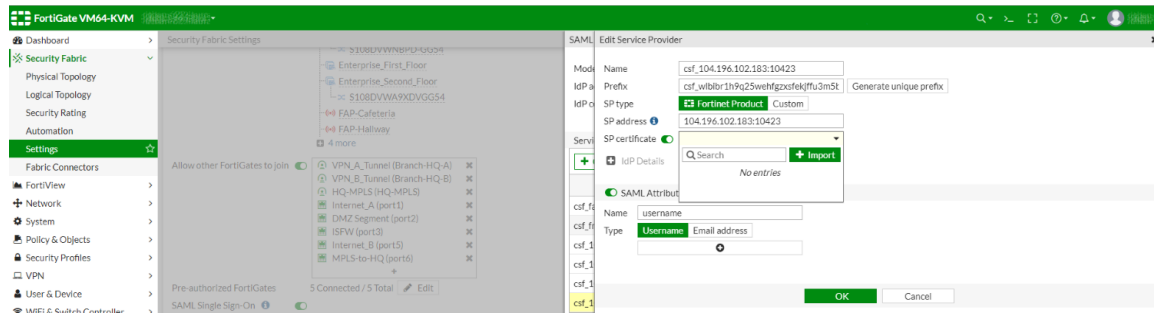
To manually import an SP certificate to an IdP:

1. Add the certificate:
 - a. On the SP, go to *Security Fabric > Settings*.
 - b. In the *FortiGate Telemetry* section, click *Advanced Options*. The *SAML SSO* pane opens.
 - c. Enable *SP certificate* and select a certificate from the dropdown box.
 - d. Click *Download*. The certificate is downloaded on the local file system.
 - e. Click *OK*.



2. Import the certificate:
 - a. On the IdP, go to *Security Fabric > Settings*.
 - b. In the *FortiGate Telemetry* section, click *Advanced Options*. The *SAML SSO* pane opens.
 - c. In the *Service Providers* table, select the SP from step 1 and click *Edit*.

- d. Enable *SP certificate* and in the dropdown box, click *Import*.



The *Upload Remote Certificate* window opens.

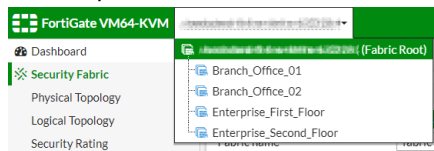
- e. Click *Upload* and select the certificate downloaded in step 1.
- f. Click *OK*. The certificate is imported.
- g. Click *OK*.
- h. In the *IdP certificate* list, select the certificate that you imported.
- i. Click *OK*.

Verifying the single-sign-on configuration

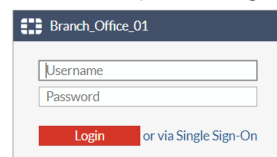
After you have logged in to a Security Fabric member using SSO, you can navigate between any Security Fabric member with SSO configured.

To navigate between Security Fabric members:

1. Log in to a Security Fabric member that is using SSO.
2. In the top banner, click the name of the device you are logged in to. A list of Security Fabric members displays.

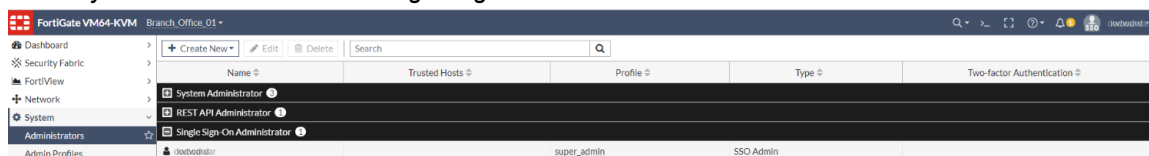


3. Click a Security Fabric member. The login page appears.
4. Select the option to log in *via Single-Sign-On*.



You are now logged in to the Security Fabric member with SSO. The letters "SSO" also display beside the user name in the top banner.

5. Go to *System > Administrators > Single-Sign-On Administrator* to view the list of SSO admins created.



CLI commands for SAML SSO

To enter a question mark (?) or a tab, Ctrl + V must be entered first. Question marks and tabs cannot be typed or copied into the CLI Console or some SSH clients.

To configure the IdP:

```
config system saml
  set status enable
  set role identity-provider
  set cert "Fortinet_Factory"
  set server-address "172.16.106.74"
  config service-providers
    edit "csf_172.16.106.74:12443"
      set prefix "csf_ngczjwqxujfsbhgr9ivhehwu37fml20"
      set sp-entity-id "http://172.16.106.74/metadata/"
      set sp-single-sign-on-url "https://172.16.106.74/saml/?acs"
      set sp-single-logout-url "https://172.16.106.74/saml/?sls"
      set sp-portal-url "https://172.16.106.74/saml/login/"
      config assertion-attributes
        edit "username"
          next
        edit "tdoc@fortinet.com"
          set type email
        next
      end
    next
  end
end
```

To configure an SP:

```
config system saml
  set status enable
  set cert "Fortinet_Factory"
  set idp-entity-id "http://172.16.106.74/saml-idp/csf_
ngczjwqxujfsbhgr9ivhehwu37fml20/metadata/"
  set idp-single-sign-on-url "https://172.16.106.74/csf_
ngczjwqxujfsbhgr9ivhehwu37fml20/login/"
  set idp-single-logout-url "https://172.16.106.74/saml-idp/csf_
ngczjwqxujfsbhgr9ivhehwu37fml20/logout/"
  set idp-cert "REMOTE_Cert_1"
  set server-address "172.16.106.74:12443"
end
```

To configure an SSO administrator:

```
config system sso-admin
  edit "SSO-admin-name"
    set accprofile <SSO admin user access profile>
    set vdom <Virtual domain(s) that the administrator can access>
  next
end
```

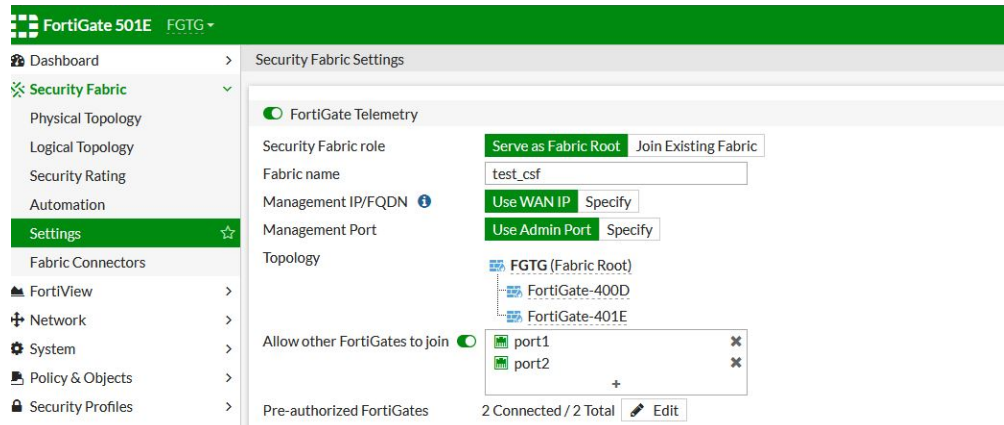
SAML SSO with pre-authorized FortiGates

You can set up SAML SSO authentication in a Security Fabric environment by starting with a root FortiGate that has one or more pre-authorized FortiGates.

After the initial configuration, you can add more downstream FortiGates to the Security Fabric, and they are automatically configured with default values for a service provider.

To set up basic SAML SSO for the Security Fabric:

1. Log in to the root FortiGate of the Security Fabric.
2. Go to *Security Fabric > Settings*, and join two pre-authorized FortiGates to the root FortiGate.



3. Configure the IdP (see [Configuring the root FortiGate as the IdP on page 120](#)).
4. Configure the SPs (see [Configuring a downstream FortiGate as an SP on page 121](#)).

Navigating between Security Fabric members with SSO

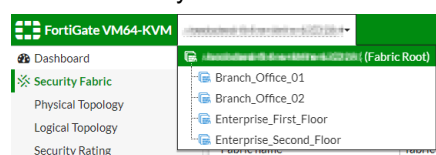
After you have logged in to a Security Fabric member by using SSO, you can navigate between any Security Fabric member with SSO configured. This can be done using the Security Fabric members dropdown menu or by logging in to a FortiGate SP from the root FortiGate IdP.

Security Fabric members dropdown

The Security Fabric members dropdown menu allows you to easily switch between all FortiGate devices that are connected to the Security Fabric. You can also use this menu to customize a FortiGate in the Security Fabric.

To navigate between Security Fabric members:

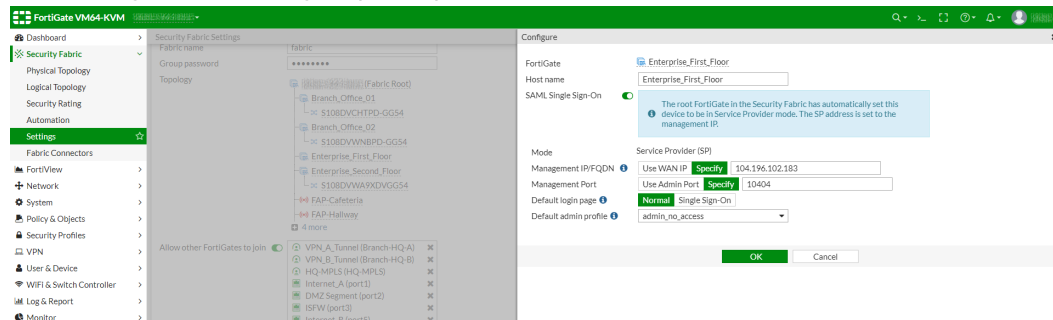
1. Log in to a Security Fabric member by using SSO.
2. In the top banner, click the name of the device you are logged into with SSO.
A list of Security Fabric members is displayed.



- Click the Security Fabric member.
You are logged in to the Security Fabric member without further authentication.

To customize a FortiGate in the Security Fabric:

- In the Security Fabric members dropdown menu, hover the cursor over a FortiGate so the tooltip is shown.
- Click *Configure*. The *Configure* pane opens.



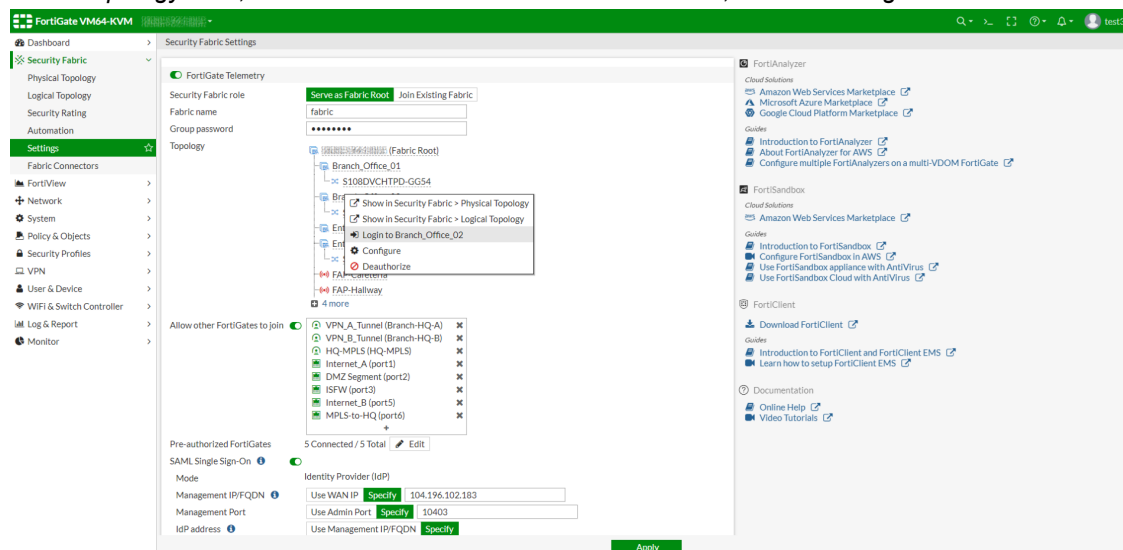
- Edit the settings as required.
- Click OK.

Logging in to an SP from the root IdP

The following example describes how to log in to a root FortiGate IdP, and navigate to other FortiGate SPs in the Security Fabric without further authentication. The local administrator account is named *test3*. The local administrator account must also be available as an SSO administrator account on all downstream FortiGate SPs. Different tabs of the same browser are used to log in to the various FortiGates.

To log in to a FortiGate SP from a root FortiGate IdP:

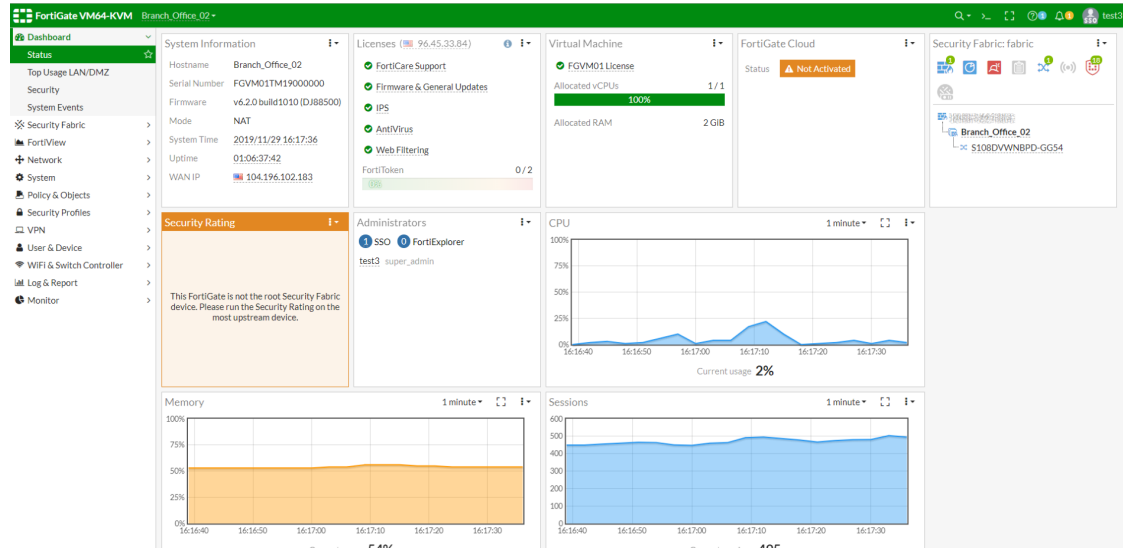
- Log in to the root FortiGate IdP by using the local administrator account.
In this example, the local administrator account is named *test3*.
- Go to *Security Fabric > Settings*.
- In the *Topology* area, click one of the downstream FortiGate SPs, and select *Login to <name of FortiGate>*.



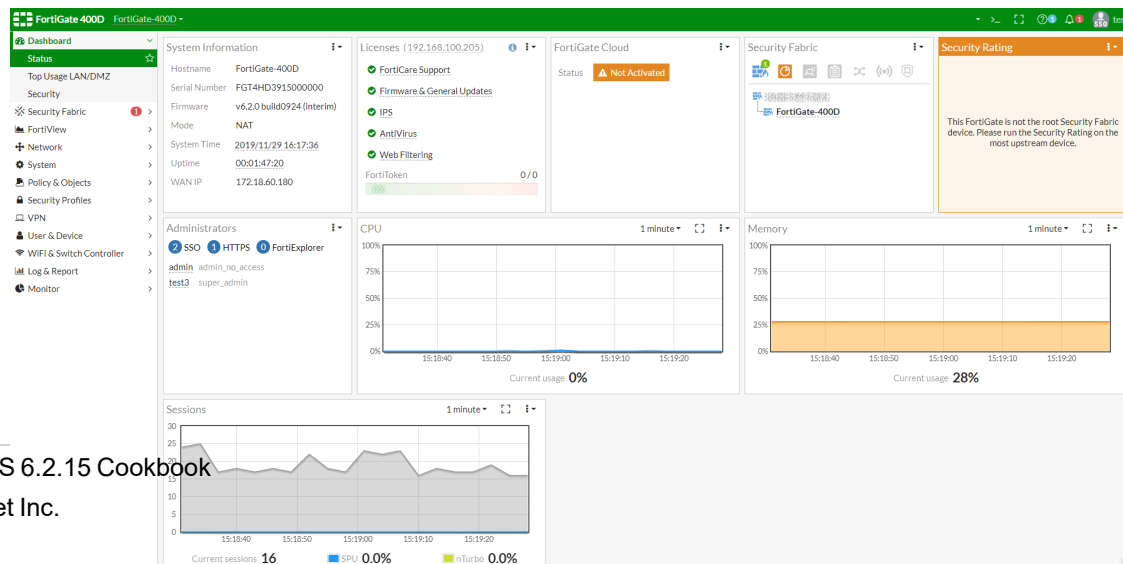
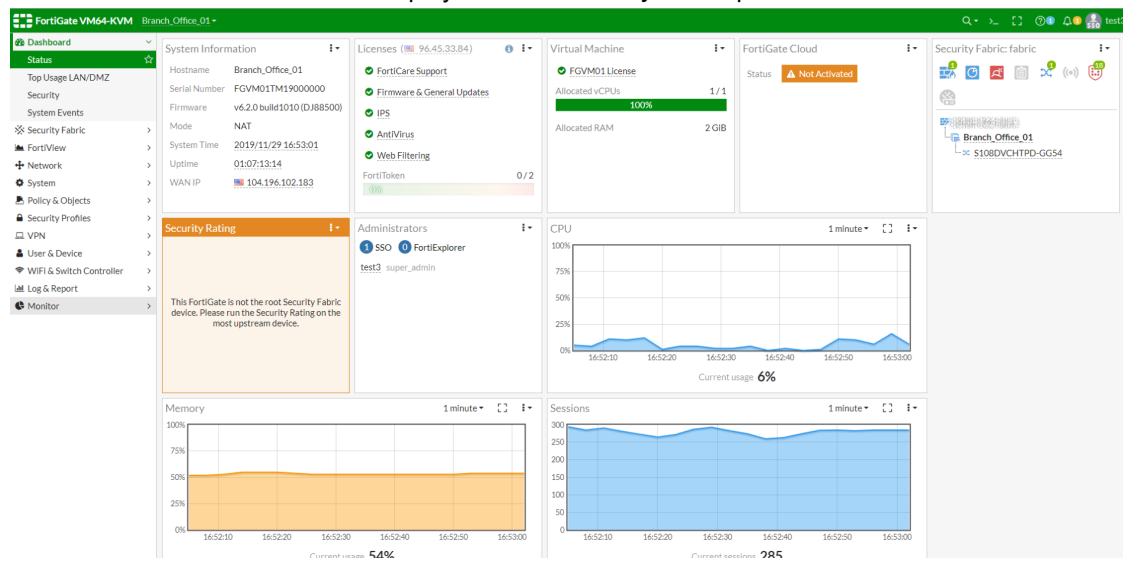
The login screen is displayed.

4. In the login screen, select **Single Sign-On**.

By using cookies in your local browser for the already-authenticated SSO administrator, FortiGate logs you in to the downstream FortiGate SP as the SSO administrator. In this example, the SSO administrator name is **test3**.



5. While still logged into the root FortiGate IdP in your browser, go to the browser tab for the root FortiGate IdP, and log in to another FortiGate SP that is displayed on the **Security Fabric** pane in the GUI.



SAML SSO login uses *SAML_IDP* session cookies of already authenticated admin users in your local browser cache to send to the root FortiGate IdP for authentication. If your browser cache is manually cleared, or you close your browser, you must authenticate again.



It is possible to log in to one downstream FortiGate SP in a Security Fabric, and then open another tab in your browser to connect to another FortiGate SP that is not a member of the Security Fabric.

This is useful in cases where the SSO administrator and the local system administrator on the FortiGate SP both have the same login name, but are two different entities.

Advanced option - FortiGate SP changes

From a root FortiGate IdP, you can edit each of the FortiGate SPs. For example, you can edit a FortiGate SP to generate a new prefix, or you can add or modify SAML attributes. When you generate a new prefix value, it is propagated to the respective downstream FortiGates.

To edit an SP from the root FortiGate (IdP):

1. Go to *Security Fabric > Settings*.
2. In the *FortiGate Telemetry* section, click *Advanced Options*. The *SAML SSO* pane opens.
3. In the *Service Providers* table, select a device, and click *Edit*. The *Edit Service Provider* pane opens.
4. Edit the settings as needed.
5. Click *OK*.

Advanced option - unique SAML attribute types

The default SAML attribute type is *username*. When the attribute type is set to *username*, SSO administrator accounts created on FortiGate SPs use the login username that is provided by the user for authentication on the root FortiGate IdP.

Because user names might not be unique, cases can occur where the user name is the same for the SSO administrator and the local administrator on the FortiGate SP. As a result, you might be unable to distinguish between actions taken by the local administrator and the SSO administrator on the FortiGate SP when looking at the system log. By using a unique SAML attribute type, such as an email address, you can create unique user names to better track what actions were taken by each administrator.

To configure a unique SAML attribute using the GUI:

1. On the root FortiGate (IdP), assign a unique email address to local administrator. In this example, the local administrator name is *test3*.
 - a. Go to *System > Administrators*, and expand the list of local users.
 - b. Select the local user, and click *Edit*.
 - c. In the *Type* field, select *Match a user on a remote server group*.
 - d. In the *Remote User Group* field, select a group.
 - e. In the *Email Address* field, enter the email address.
 - f. Click *OK*.

The screenshot shows the FortiGate 501E GUI with the 'Edit Administrator' configuration page. The left sidebar shows the navigation menu with 'System' and 'Administrators' highlighted. The main content area shows the configuration for a user named 'test3'. The 'Type' dropdown is open, showing the following options: 'Local User', 'Match a user on a remote server group' (which is highlighted), 'Match all users in a remote server group', and 'Use public key infrastructure (PKI) group'. The 'Email Address' field is set to 'ooooo@fortinet.com'. Other fields include 'Username' (test3), 'Administrator Profile' (super_admin), and 'Remote User Group' (Idap). There are also checkboxes for 'SMS', 'Two-factor Authentication', 'Restrict login to trusted hosts', and 'Restrict admin to guest account provisioning only'. At the bottom right, there are 'OK' and 'Cancel' buttons.

2. On the root FortiGate (IdP), update the SAML configuration:
 - a. Go to *Security Fabric > Settings*.
 - b. In the *FortiGate Telemetry* section, click *Advanced Options*. The *SAML SSO* pane opens.
 - c. In the *Service Providers* table, select the FortiGate, and click *Edit*. The *Edit Service Provider* pane opens.
 - d. For *SP type*, select *Custom*.
 - e. In the *SAML Attribute* section for *Type*, select *Email address*.
 - f. Beside *Type*, select *Email address*.
 - g. Click *OK*.

FortiGate 401E FGT_A

Edit Service Provider

Name: FGTA-184

Prefix: 3dktfoqgbxtldbts

SP type: Fortinet Product Custom

SP portal URL: https://172.18.60.184/saml/login/

SP entity ID: http://172.18.60.184/metadata/

SP ACS (login) URL: https://172.18.60.184/saml/acs

SP SLS (logout) URL: https://172.18.60.184/saml/ls

SP certificate: ☐

IdP Details

SAML Attribute

Name: username

Type: Username Email address

OK Cancel

After the administrator (test3) logs in to the FortiGate SP for the first time, SAML authentication occurs on FortiGate SP. A new SSO administrator account is created, and the account name is now the email address instead of the login name (test3).

To view the new SSO administrator account:

- In the SP, go to *System > Administrators*, and expand the list of SSO administrators. The email address (ooooo@fortinet.com) is listed as the account name:

Name	Trusted Hosts	IPv6 Trusted Host	Profile	Type	Virtual Domain	Two-factor Authentication
admin			super_admin	Local	Global	Disabled
ftm			super_admin	Local	Global	FTKMOB947EEF73CD
g-admin			super_admin	Local	Global	Disabled
remote-admin			super_admin	Remote+Wildcard	Global	Disabled
test3			super_admin	Remote User	Global	Disabled
Single Sign-On Administrator						
ooooo@fortinet.com			super_admin	SSO Admin	Global	

If the SAML attribute had been set to the default setting of *username*, the user name for the SSO administrator account would have been (test3).

To view the SSO administrator activity in the log files:

- In the SP, go to *Log & Report > Events*. Because the SAML attribute is set to *Custom*, the SSO administrator account ooooo@fortinet.com is used as the user name on the FortiGate SP, and it appears in the log files:

Date/Time	Level	User	Message	Log Description
2019/06/21 09:56:19	Info	ooooo@fortinet.com	Edit system.sso-admin ooooo@fortinet.com	Object attribute configured
2019/06/21 09:55:46	Info	ooooo@fortinet.com	Administrator ooooo@fortinet.com logged in successfully from sso[10.1.100.254]	Admin login successful
2019/06/21 09:52:28	Info		Delete 1 old report files	Outdated report files deleted
2019/06/21 09:47:28	Info		Delete 1 old report files	Outdated report files deleted

To configure a unique SAML attribute using the CLI:

```

config system saml
  set status enable
  set role identity-provider
  set cert "fgt_g_san_extern_new"
  set server-address "172.18.60.187"
  config service-providers
    edit "csf_172.18.60.185"
      set prefix "csf_avju0tk4oioidifz3kbh2fms8dw688hn"
      set sp-entity-id "http://172.18.60.185/metadata/"
      set sp-single-sign-on-url "https://172.18.60.185/saml/?acs"
      set sp-single-logout-url "https://172.18.60.185/saml/?sls"
      set sp-portal-url "https://172.18.60.185/saml/login/"
      config assertion-attributes
        edit "username"
        next
      end
    next
    edit "FGTA-180"
      set prefix "yxs8uhq47b5b2urq"
      set sp-entity-id "http://172.18.60.180/metadata/"
      set sp-single-sign-on-url "https://172.18.60.180/saml/?acs"
      set sp-single-logout-url "https://172.18.60.180/saml/?sls"
      set sp-portal-url "https://172.18.60.180/saml/login/"
      config assertion-attributes
        edit "username"
        next
      end
    next
    edit "FGTA-184"
      set prefix "3dktfo0gbxtldbts"
      set sp-entity-id "http://172.18.60.184/metadata/"
      set sp-single-sign-on-url "https://172.18.60.184/saml/?acs"
      set sp-single-logout-url "https://172.18.60.184/saml/?sls"
      set sp-portal-url "https://172.18.60.184/saml/login/"
      config assertion-attributes
        edit "username"
        set type email
        next
      end
    next
  end
end

```

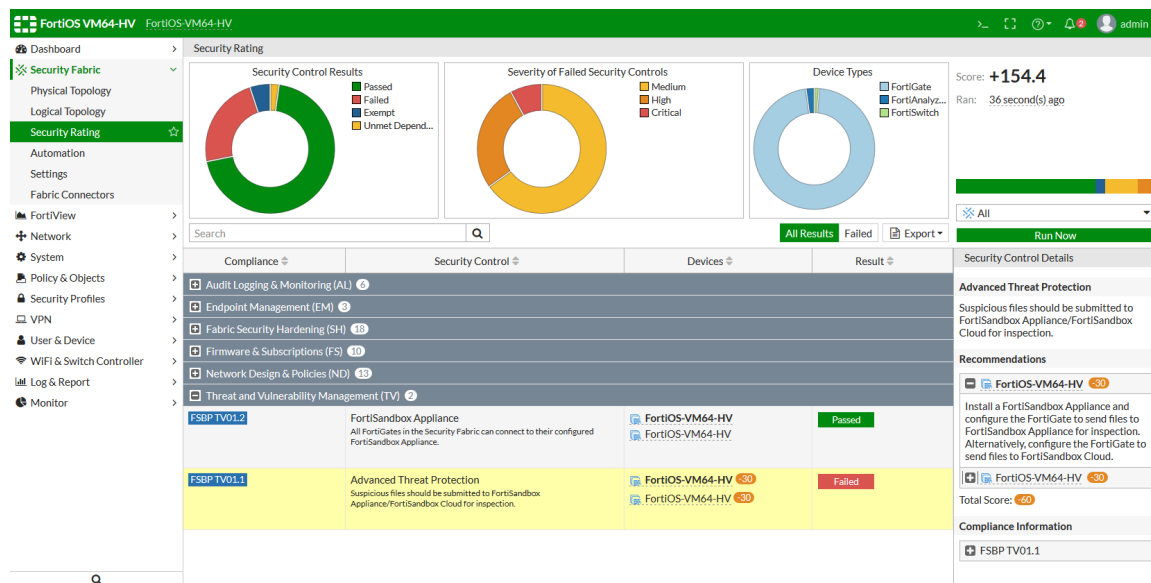
The `csf_172.18.60.185` service provider was automatically added when the FortiGate SP 172.18.60.185 joined the root FortiGate IdP in the Security Fabric.

All `sp-*` options, such as `sp-portal-url`, are set with default values when a service provider is created, but can be modified using the CLI or GUI.

Security rating

The security rating analyzes your Security Fabric deployment, identifies potential vulnerabilities, highlights best practices that can be used to improve the security and performance of your network, and calculates Security Fabric scores.

To view the security rating and run a security rating check, go to *Security Fabric > Security Rating* on the root FortiGate. Click *Run Now* to run a security rating check. Checks can also be run automatically every four hours.



The security rating check uses real-time monitoring to analyze the network based on the current network configuration. When the check is complete, the results table shows a list of the checks that were performed, including:

- The name and a description of the check.
- The device or devices that the check was performed on.
- The impact of the check on the overall security score.
- The check results—whether it passed or failed.

The list can be searched, filtered to show all results or only failed checks, and exported to a CSV or JSON file. Clicking a color or legend name in the donut charts will also filter the results.

Hovering the cursor over a check result score will show the breakdown of how that score was calculated.

Selecting a specific check from the list shows details about that check in the *Security Control Details* pane, including recommendations and compliance information. For failed checks, this includes a description of what remediation actions could be taken. For recommendations that support *Easy Apply*, the device will have an *EZ* symbol next to its name, and the remediation action can be taken automatically by clicking *Apply* under the recommendations. See [Comprehensive report extensions on page 135](#) for more information about security rating reports.

For more information about security ratings, including details about each check that is performed, go to [Security Best Practices & Security Rating Feature](#).



Security rating licenses are required to run security rating checks across all the devices in the Security Fabric. It also allows ratings scores to be submitted to and received from FortiGuard for ranking networks by percentile.

See <https://www.fortinet.com/support/support-services/fortiguard-security-subscriptions/security-rating.html> for information.

Automatic security rating checks

Security rating checks can be scheduled to run automatically every four hours.

To enable automatic security checks using the CLI:

```
config system global
    security-rating-run-on-schedule {enable | disable}
end
```

Opt out of ranking

Security rating scores can be submitted to FortiGuard for comparison with other organizations' scores, allowing a percentile score to be calculated. If you opt out of submitting your score, only an absolute score will be available.

To opt out of submitting the score using the CLI:

```
config system global
    set security-rating-result-submission {enable | disable}
end
```

Logging the security rating

The results of past security checks are available in *Log & Report > Events* and selecting *Security Rating Events* from the event type dropdown list.

Date/Time	Level	Log Description	Result	Security Score
2019/05/08 23:29:57	Info	Security Rating summary	1 20 0 0 76	+69.6
2019/05/08 23:23:19	Info	Security Rating summary	1 20 0 0 76	+69.6
2019/05/08 19:18:42	Info	Security Rating summary	1 22 15 0 118	-26.9
2019/05/08 15:12:39	Info	Security Rating summary	1 12 0 0 61	+147
2019/05/08 11:05:46	Info	Security Rating summary	0 0 0 0 40	+277.5
2019/05/07 18:01:57	Info	Security Rating summary	2 12 0 0 76	+154.4
2019/05/07 18:01:19	Info	Security Rating summary	2 12 0 0 76	+154.4
2019/05/07 17:33:23	Info	Security Rating summary	2 12 0 0 76	+154.4
2019/05/07 13:27:58	Info	Security Rating summary	1 12 0 0 61	+159.3
2019/05/06 11:39:48	Info	Security Rating summary	1 15 11 0 60	+104.4
2019/05/06 11:38:48	Info	Security Rating summary	1 15 15 0 76	+22.1
2019/05/06 11:38:20	Info	Security Rating summary	1 15 15 0 76	+4.7
2019/05/06 11:10:40	Info	Security Rating summary	1 7 5 0 50	+122.5

Log Details

General

Date: 2019/05/07
Time: 18:01:57
Virtual Domain: root
Log Description: Security Rating summary

Security

Level: Info

Security Rating

Security Ranking ID: 1557277287
Security Rating Time: 1557277317
Security Score: +154.4
Critical Count: 2
High Count: 7
Medium Count: 40
Low Count: 0
Passed Count: 76

Other

Sub Type: security-rating
Log event original timestamp: 1557277317

An event filter subtype can be created for the Security Fabric rating so that event logs are created on the root FortiGate that summarize the results of a check, and show detailed information for the individual tests.

To configure security rating logging using the CLI:

```
config log eventfilter
    set security-rating enable
end
```

Security Fabric score

The Security Fabric score is calculated when a security rating check is run, based on the severity level of the checks that are passed or failed. A higher scores represents a more secure network. Points are added for passed checks and removed for failed checks.

Severity level	Weight (points)
Critical	50
High	25
Medium	10
Low	5

To calculate the number of points awarded to a device for a passed check, the following equation is used:

$$\text{score} = \frac{\text{<severity level weight>}}{\text{<\# of FortiGates>}} \times \text{<secure FortiGate multiplier>}$$

The secure FortiGate multiplier is determined using logarithms and the number of FortiGate devices in the Security Fabric.

For example, if there are four FortiGate devices in the Security Fabric that all pass the compatible firmware check, the score for each FortiGate device is calculated with the following equation:

$$\frac{50}{4} \times 1.292 = 16.15 \text{ points}$$

All of the FortiGate devices in the Security Fabric must pass the check in order to receive the points. If any one of the FortiGate devices fails a check, the devices that passed are not awarded any points. For the device that failed the check, the following equation is used to calculated the number of points that are lost:

$$\text{score} = \text{<severity level weight>} \times \text{<secure FortiGate multiplier>}$$

For example, if the check finds two critical FortiClient vulnerabilities, the score is calculated with the following equation:

$$-50 \times 2 = -100 \text{ points}$$

Scores are not affected by checks that do not apply to your network. For example, if there are no FortiAP devices in the Security Fabric, no points will be added or subtracted for the FortiAP firmware version check.

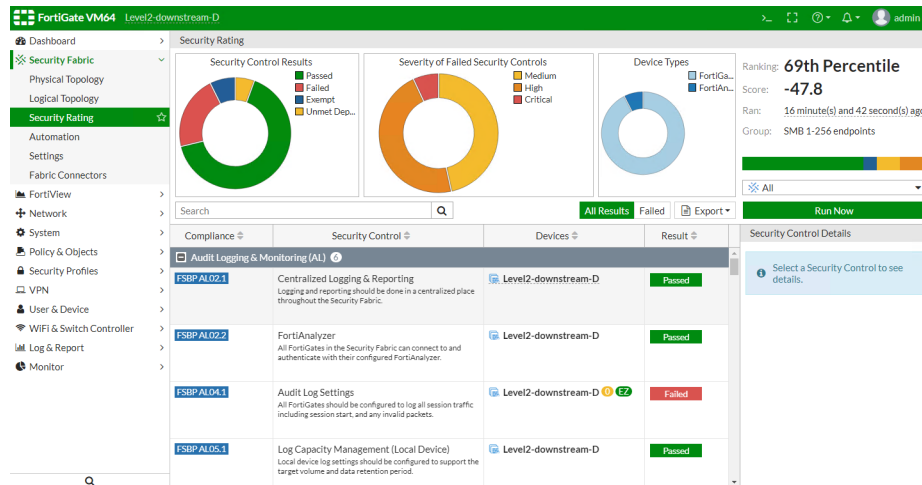
Comprehensive report extensions

Security rating reports include the following:

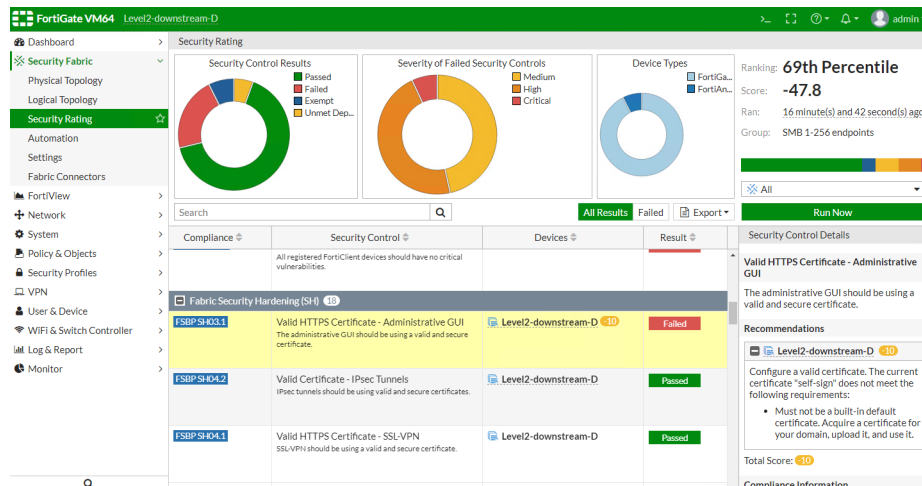
- Summary charts along the top. You can click a chart for easy filtering.
- Grouping common rating checks across multiple devices in a single entry.
- The right frame summarizes all information for the single check.
- You can apply recommendations from within the right frame (*Easy Apply*).
- You can choose to show full results or subsets, such as failed only.

Sample report views

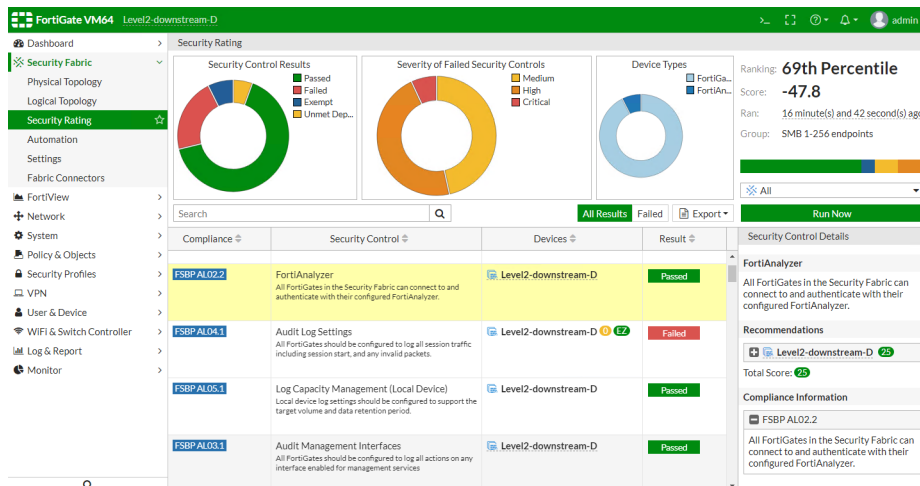
The default view for the *Security Rating* report:



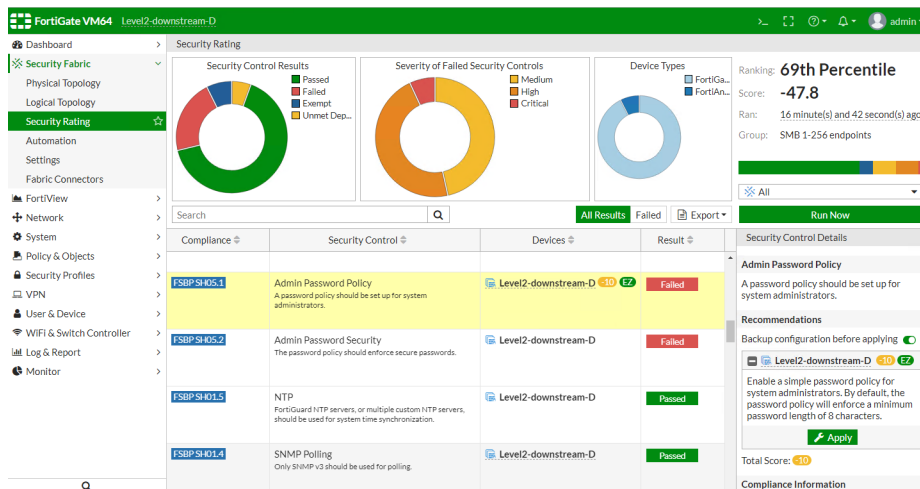
Security Rating report with a specific test selected:



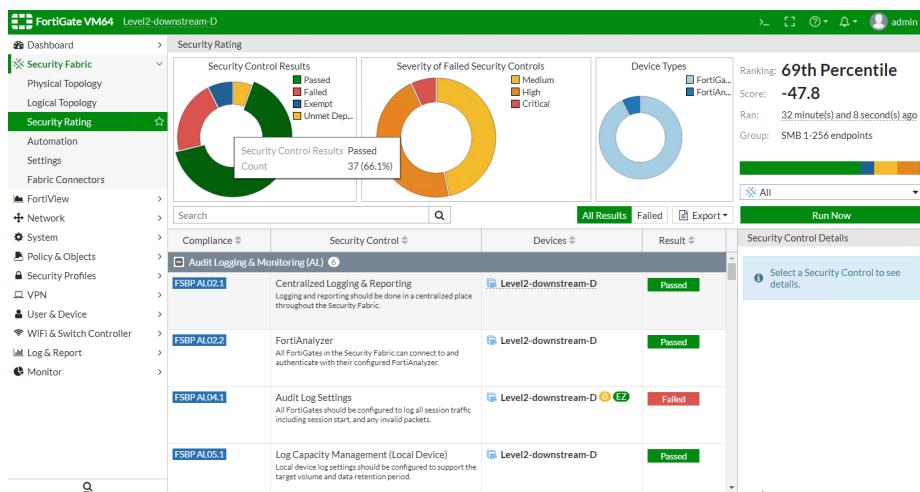
Additional details for each compliance test:



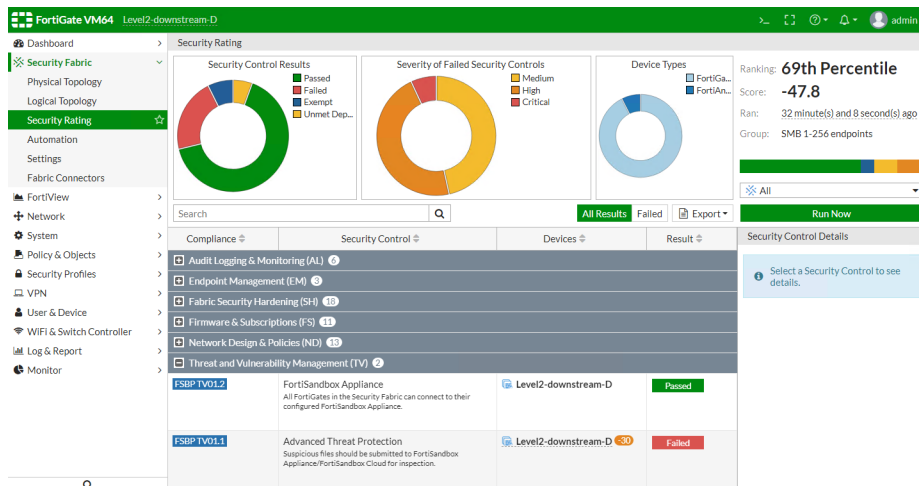
You can select *Easy Apply (EZ)* for individual recommendations:



Security Rating report summary:



Security Rating report with full results, including passed and failed tests:

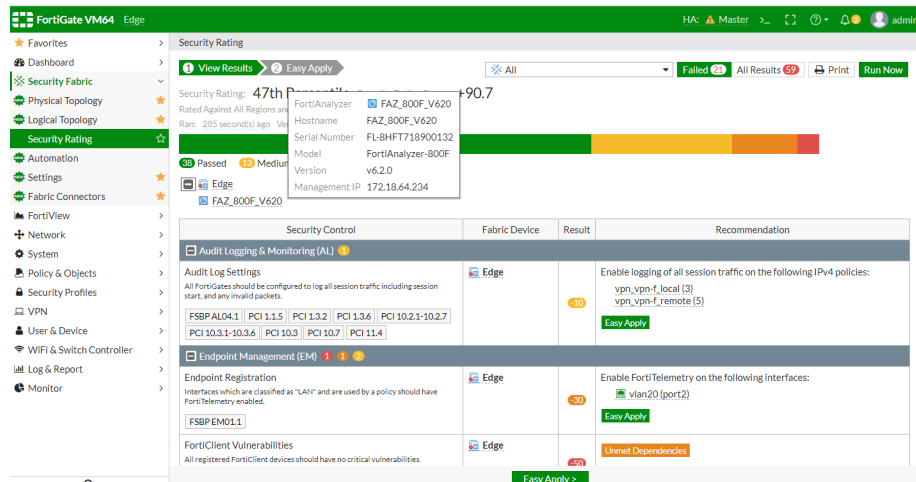


Verifying FortiAnalyzer configurations

The *Security Rating* report can verify FortiAnalyzer configurations and displays the results in the *Compatible Firmware* and *Admin Idle Timeout* tests.

To view FortiAnalyzer information and tests:

1. Go to *Security Fabric > Security Rating*.
2. The *Security Rating* results page displays the FortiAnalyzer icon in the topology field, and FortiAnalyzer information is available through the tooltip.



3. The *Compatible Firmware* and *Admin Idle Timeout* tests for FortiAnalyzer are now available.

- **Compatible Firmware:**

The screenshot shows the FortiGate VM64 Security Rating dashboard. The left sidebar contains navigation options: Favorites, Dashboard, Security Fabric (selected), Physical Topology, Logical Topology, Security Rating (selected), Automation, Settings, Fabric Connectors, FortiView, Network, System, Policy & Objects, Security Profiles, VPN, User & Device, WIFI & Switch Controller, Log & Report, and Monitor. The main panel displays the Security Rating for the 'Edge' device. The 'View Results' tab is active, showing a Security Rating Score of +90.7 (47th Percentile). A bar chart shows the distribution of scores: 10 Passed, 13 Medium, 4 High, and 2 Critical. Below the chart, a table lists security controls and their results:

Security Control	Fabric Device	Result	Recommendation
Audit Logging & Monitoring (AL) 4			
Endpoint Management (EM) 1 1 2			
Fabric Security Hardening (SH) 4 8 7			
Firmware & Subscriptions (FS) 13			
Compatible Firmware All devices in the Security Fabric should have compatible firmware versions.	Edge	27/2	--
FSBPFS01.1	FAZ_800F_V620	27/2	--
FortiAP Firmware Versions All FortiAPs should be running the latest firmware.	Edge	10	--
FSBPFS01.2			
FortiSwitch Firmware Versions All FortiSwitches should be running the latest firmware.	Edge	10	--

An 'Easy Apply' button is visible at the bottom right of the table.

- **Admin Idle Timeout:**

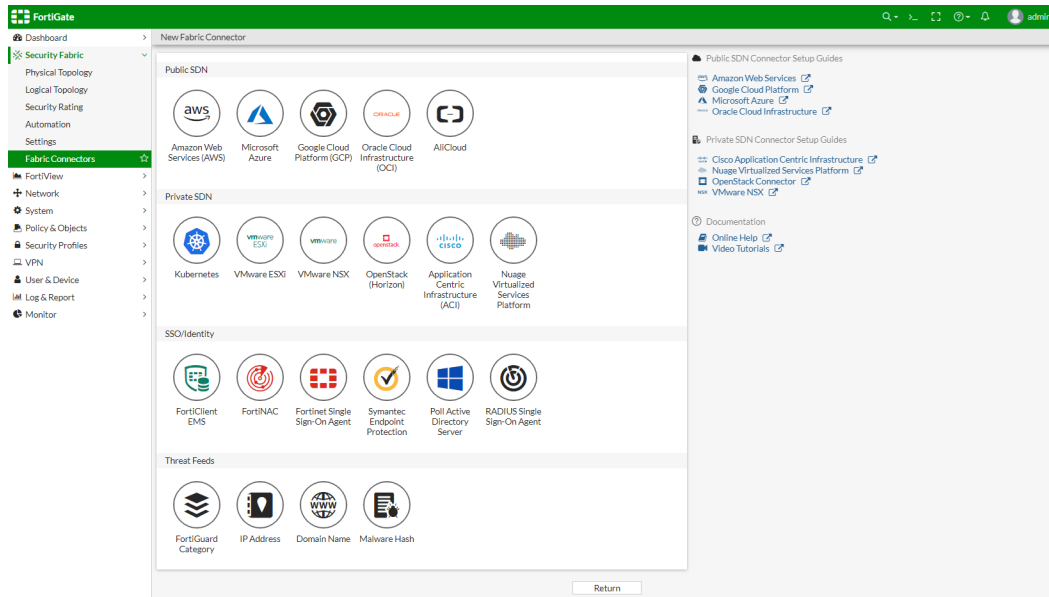
The screenshot shows the FortiGate VM64 Security Rating dashboard with the 'Admin Idle Timeout' test results. The left sidebar is the same as the previous screenshot. The main panel displays the Security Rating for the 'Edge' device. The 'View Results' tab is active, showing a Security Rating Score of +90.7 (47th Percentile). A bar chart shows the distribution of scores: 10 Passed, 13 Medium, 4 High, and 2 Critical. Below the chart, a table lists security controls and their results:

Security Control	Fabric Device	Result	Recommendation
Admin Idle Timeout The timeout for idle administrators should be at most 15 minutes.	Edge	10	Modify the timeout for idle administrators to be at most 15 minutes.
FSBP SH09.1 PCI 8.1.8	FAZ_800F_V620	10	Modify the timeout for idle administrators to be at most 15 minutes.
Failed Login Attempts The administrator lockout threshold should be at most 3 attempts, and the lockout duration at least 15 minutes.	Edge	10	Apply the following requirement(s): • Lockout duration should be at least 15 minutes.
FSBP SH09.2			
Two Factor Authentication Every administrator should have two factor authentication enabled.	Edge	20	Enable two factor authentication for the following administrators: • admin • admin1 • admin2 • readonly • test3
FSBP SH09.5			
FortiGate Identification All FortiGates should have a unique hostname set.	Edge	10	--
FSBP SH14.1			
USB Auto Configuration Automatic USB firmware and configuration provisioning features should be disabled during normal operation.	Edge	20	--
FSBP SH15.1			
Firmware & Subscriptions (FS) 13			
Network Design & Policies (ND) 2 14			

An 'Easy Apply' button is visible at the bottom right of the table.

Fabric connectors

Fabric connectors allow you to connect your network to external services. Following are the categories of connectors: Public SDN, Private SDN, SSO/Identity, and Threat Feeds.



If VDOMs are enabled, SDN and Threat Feeds connectors are in the global settings, and SSO/Identity connectors are per VDOM.

SDN connectors

Fabric connectors to SDNs provide integration and orchestration of Fortinet products with SDN solutions. Fabric Connectors ensure that any changes in the SDN environment are automatically updated in your network.

There are four steps to creating and using an SDN connector:

1. Gather the required information
2. [Create the fabric connector on page 140](#)
3. [Create a fabric connector address on page 141](#)
4. [Add the address to a firewall policy on page 142](#)

An example of creating a Microsoft Azure SDN connector is available at [Configuring a Fabric connector in Azure](#).

Create the fabric connector

To create an SDN Fabric connector in the GUI:

1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New*.
3. Click on the service that you are using.
4. Enter the *Name*, *Status*, and *Update Interval* for the connector.
5. Enter the previously collected information for the specific connector that you are creating.
6. Click *OK*.

To create an SDN Fabric connector in the CLI:

```
config system sdn-connector
  edit <name>
    set status {enable | disable}
    set type {connector type}
    ...
    set update-interval <integer>
  next
end
```



The available CLI commands will vary depending on the selected SDN connector type.

Create a fabric connector address

A fabric connector address can be used in the following ways:

- As the source or destination address for firewall policies.
- To automatically update changes to addresses in the environment of the service that you are using, based on specified filtering conditions.
- To automatically apply changes to firewall policies that use the address, based on specified filtering conditions.

To create a fabric connector address in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address*.
3. Enter a name for the address.
4. Set the *Type* to *Fabric Connector Address*.
5. Select an *SDN Connector* from the drop-down list, or click *Create New* to make a new one.
6. Set the *SDN address type*. Only addresses of the selected type will be collected.
7. Configure the connector specific settings.
8. Select an *Interface* for the address, or leave it as *any*, enable or disable *Show in Address List*, and optionally add *Comments*.
9. Add tags.
10. Click *OK*.

To create a fabric connector address in the CLI:

```
config firewall address
  edit <name>
    set type dynamic
    set sdn <sdn_connector>
    set visibility enable
    set associated-interface <interface_name>
    set color <integer>
    ...
    set comment <comment>
  config tagging
```

```
        edit <name>
            set category <string>
            set tags <strings>
        next
    end
next
end
```



The available CLI commands will vary depending on the selected SDN connector type.

Add the address to a firewall policy

A fabric connector address can be used as either the source or destination address.

To add the address to a firewall policy in the GUI:

1. Go to *Policy & Objects > IPv4 Policy*.
2. Click *Create New*.
3. Enter a name for the policy.
4. Set the incoming and outgoing interfaces.
5. Use the fabric connector address as the source or destination address.
6. Configure the remaining settings as needed.
7. Click *OK*.

To add the address to a firewall policy in the CLI:

```
config firewall policy
    edit 0
        set name <name>
        set srcintf <port_name>
        set dstintf <port_name>
        set srcaddr <firewall_address>
        set dstaddr <firewall_address>
        set action accept
        set schedule <schedule>
        set service <service>
    next
end
```

AliCloud SDN connector

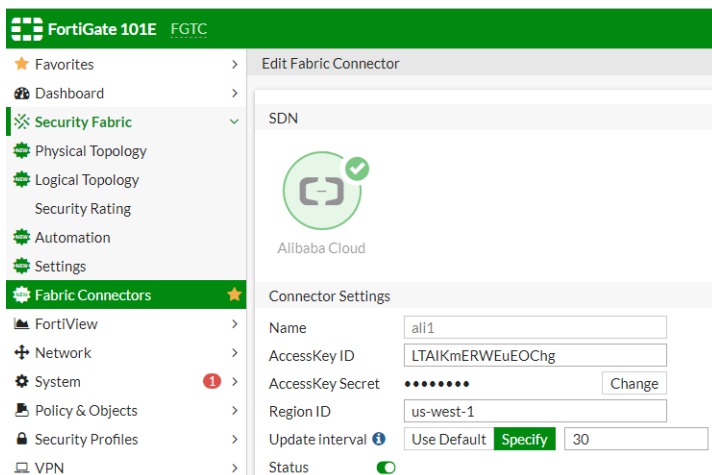
FortiOS automatically updates dynamic addresses for AliCloud using an AliCloud SDN connector, including mapping the following attributes from AliCloud instances to dynamic address groups in FortiOS:

- ImageId
- InstanceId
- SecurityGroupId
- VpcId

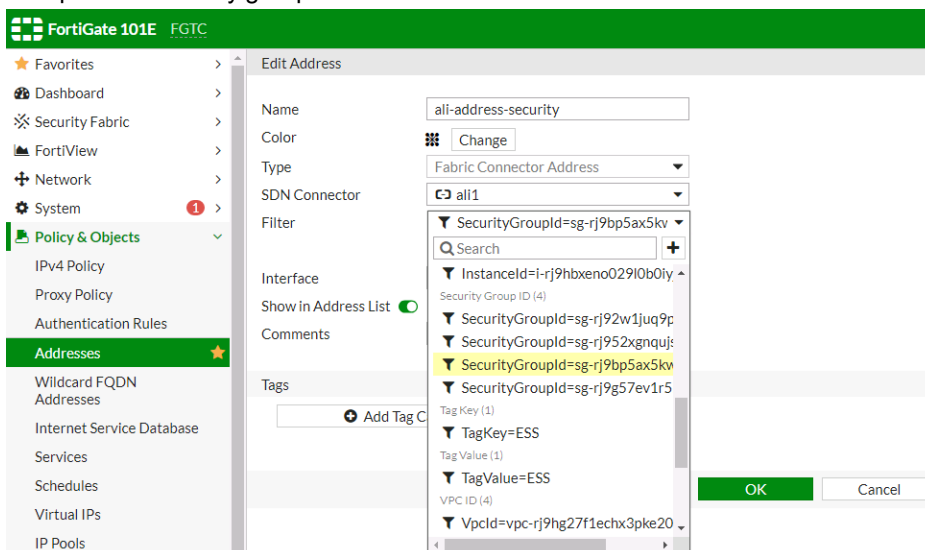
- VSwitchId
- TagKey
- TagValue

To configure AliCloud SDN connector using the GUI:

1. Configure the AliCloud SDN connector:
 - a. Go to *Security Fabric > Fabric Connectors*.
 - b. Click *Create New*, and select *Alibaba Cloud*.
 - c. Configure as shown, substituting the access key, secret, and region ID for your deployment. The update interval is in seconds.

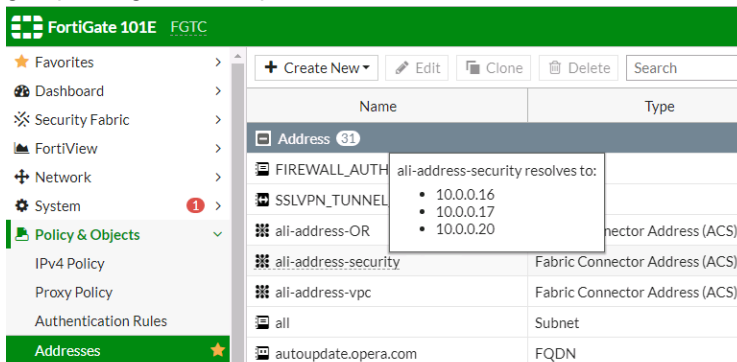


2. Create a dynamic firewall address for the configured AliCloud SDN connector:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Click *Create New*, then select *Address*.
 - c. Configure the address as shown, selecting the desired filter in the *Filter* dropdown list. In this example, the AliCloud SDN connector will automatically populate and update IP addresses only for instances that belong to the specified security group:



3. Ensure that the AliCloud SDN connector resolves dynamic firewall IP addresses:

- a. Go to *Policy & Objects > Addresses*.
- b. Hover over the address created in step 2 to see a list of IP addresses for instances that belong to the security group configured in step 2:



To configure AliCloud SDN connector using CLI commands:

1. Configure the AliCloud SDN connector:

```
config system sdn-connector
  edit "ali1"
    set type acs
    set access-key "LTAIKmERWEuEOChg"
    set secret-key xxxxx
    set region "us-west-1"
    set update-interval 30
  next
end
```

2. Create a dynamic firewall address for the configured AliCloud SDN connector with the supported AliCloud filter. In this example, the AliCloud SDN Connector will automatically populate and update IP addresses only for instances that belong to the specified security group:

```
config firewall address
  edit "ali-address-security"
    set type dynamic
    set sdn "ali1"
    set filter "SecurityGroupId=sg-rj9bp5ax5kwy3gqdzqb"
  next
end
```

3. Confirm that the AliCloud SDN connector resolves dynamic firewall IP addresses using the configured filter:

```
config firewall address
  edit "ali-address-security"
    set uuid 62a76df2-18f6-51e9-b555-360b18359ebe
    set type dynamic
    set sdn "ali1"
    set filter "SecurityGroupId=sg-rj9bp5ax5kwy3gqdzqb"
    config list
      edit "10.0.0.16"
      next
      edit "10.0.0.17"
      next
      edit "10.0.0.20"
      next
    end
```

next
end

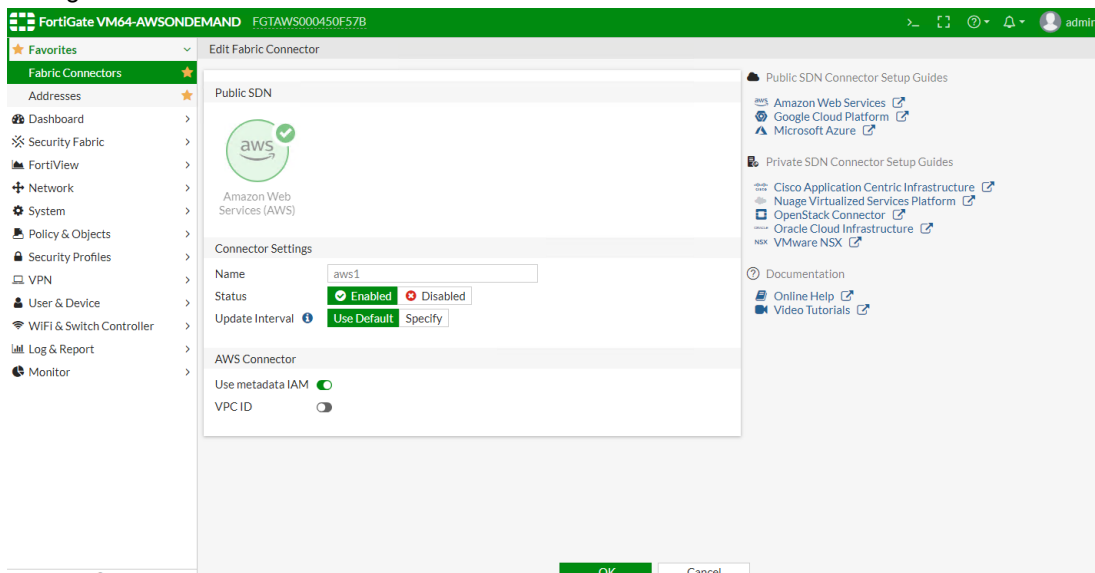
AWS SDN connector with IAM credentials

For instances running in AWS (on demand or BYOL), you can set up the AWS SDN connector using AWS Identify and Access Management (IAM) credentials.

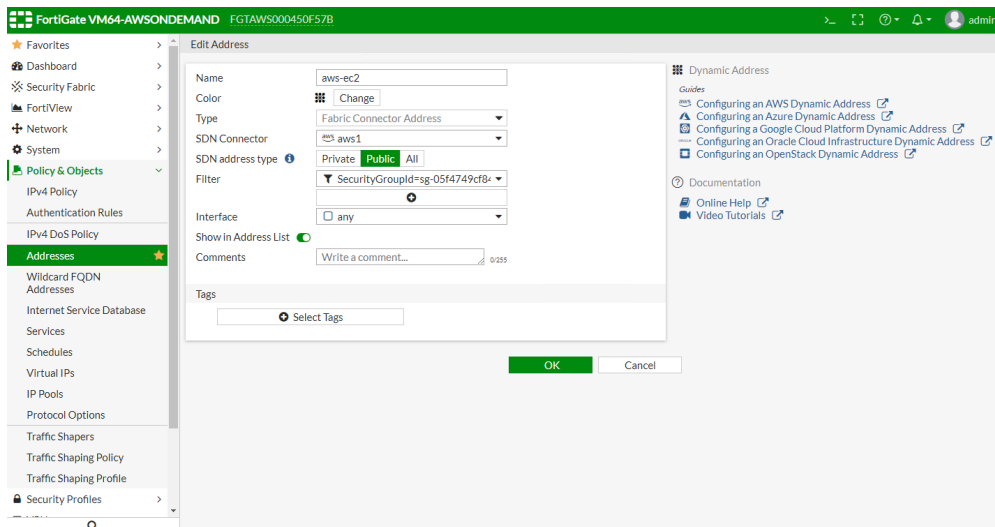
IAM authentication is available only for FGT-AWS and FGT-AWSONDEMAND platforms.

To configure AWS SDN connector using the GUI:

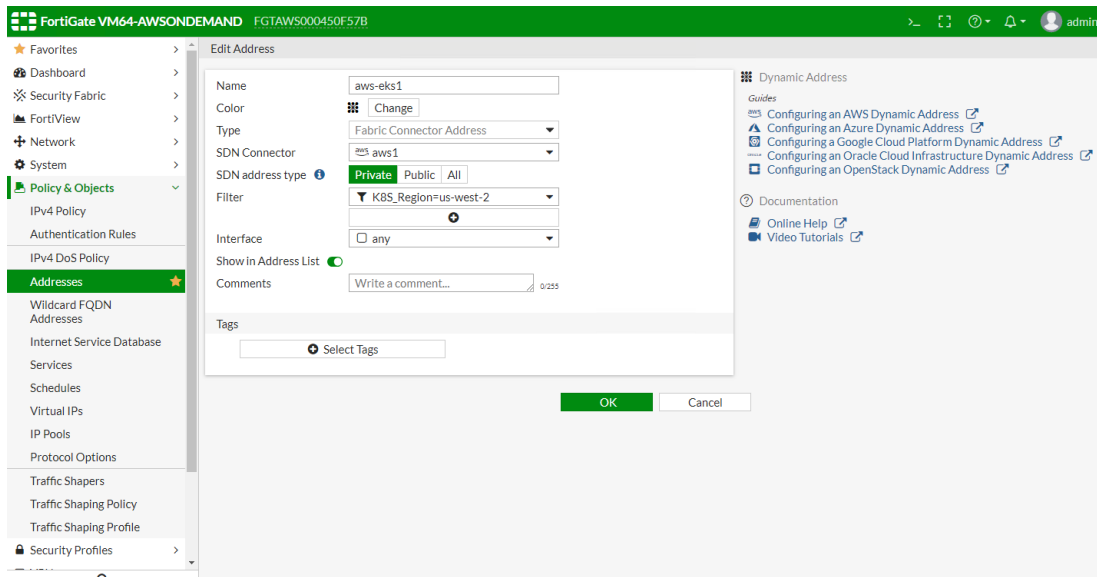
1. Configure the AWS SDN connector:
 - a. Go to *Security Fabric > Fabric Connectors*.
 - b. Click *Create New*, and select *Amazon Web Services (AWS)*.
 - c. Configure as shown:



2. Create a dynamic firewall address for the configured AWS SDN connector:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Click *Create New*, then select *Address*.
 - c. Configure the address as shown, selecting the desired filter in the *Filter* dropdown list.
Following is an example for a public SDN address type:



Following is an example for a private SDN address type:



3. Ensure that the AWS SDN connector resolves dynamic firewall IP addresses:

- a. Go to *Policy & Objects > Addresses*.
- b. Hover over the address created in step 2 to see a list of IP addresses for instances that belong to the security group configured in step 2.

Following is an example for a public SDN address type:

Name	Type	Details	Interface	Visibility	Ref.
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL	Subnet	0.0.0.0/0		Hidden	0
SSLVPN	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	2
all	Subnet	0.0.0.0/0		Visible	0
aws-ec2	Fabric Connector Address (AWS)			Visible	1
aws-eks1	Fabric Connector Address (AWS)			Visible	1
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
none	Subnet	0.0.0.0/32		Visible	0

Following is an example for a private SDN address type:

Name	Type	Details	Interface	Visibility	Ref.
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL	Subnet	0.0.0.0/0		Hidden	0
SSLVPN	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	2
all	Subnet	0.0.0.0/0		Visible	0
aws-ec2	Fabric Connector Address (AWS)			Visible	1
aws-eks1	Fabric Connector Address (AWS)			Visible	1
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
none	Subnet	0.0.0.0/32		Visible	0

To configure AWS SDN connector using CLI commands:

1. Configure the AWS connector:

```
config system sdn-connector
edit "aws1"
set status enable
set type aws
set use-metadata-iam enable
set update-interval 60
next
end
```

2. Create a dynamic firewall address for the configured AWS SDN connector with the supported filter:

Dynamic firewall address IPs are resolved by the SDN connector.

```
config firewall address
```

```
edit "aws-ec2"
  set type dynamic
  set sdn "aws1"
  set filter "SecurityGroupId=sg-05f4749cf84267548"
  set sdn-addr-type public
next
edit "aws-eks1"
  set type dynamic
  set sdn "aws1"
  set filter "K8S_Region=us-west-2"
next
end
```

3. Confirm that the AWS SDN connector resolves dynamic firewall IP addresses using the configured filter:

```
config firewall address
  edit "aws-ec2"
    set uuid e756e786-3a2e-51e9-9d40-9492098de42d
    set type dynamic
    set sdn "aws1"
    set filter "SecurityGroupId=sg-05f4749cf84267548"
    set sdn-addr-type public
    config list
      edit "34.222.246.198"
      next
      edit "54.188.139.177"
      next
      edit "54.218.229.229"
      next
    end
  next
  edit "aws-eks1"
    set uuid d84589aa-3a10-51e9-b1ac-08145abce4d6
    set type dynamic
    set sdn "aws1"
    set filter "K8S_Region=us-west-2"
    config list
      edit "192.168.114.197"
      next
      edit "192.168.167.20"
      next
      edit "192.168.180.72"
      next
      edit "192.168.181.186"
      next
      edit "192.168.210.107"
      next
    end
  next
end
```

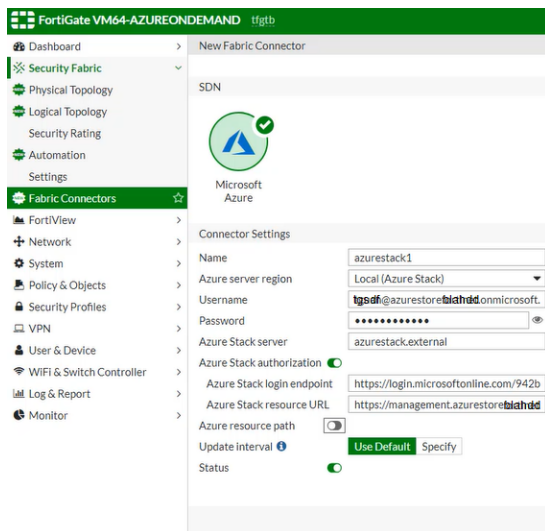
Azure Stack SDN connector

FortiOS automatically updates dynamic addresses for Azure Stack on-premise environments using an Azure Stack SDN connector, including mapping the following attributes from Azure Stack instances to dynamic address groups in FortiOS:

- vm
- tag
- size
- securitygroup
- vnet
- subnet
- resourcegroup
- vmss

To configure Azure Stack SDN connector using the GUI:

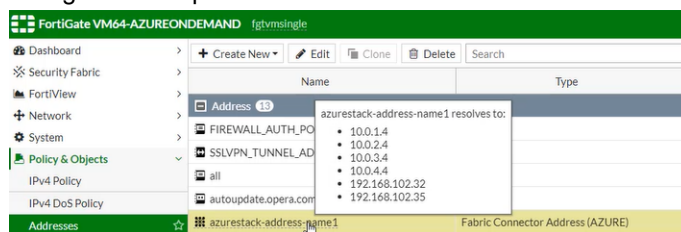
1. Configure the Azure Stack SDN connector:
 - a. Go to *Security Fabric > Fabric Connectors*.
 - b. Click *Create New*, and select *Microsoft Azure*.
 - c. Configure as shown, substituting the Azure Stack settings for your deployment. The update interval is in seconds.



2. Create a dynamic firewall address for the configured Azure Stack SDN connector:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Click *Create New*, then select *Address*.
 - c. Configure the address as shown, selecting the desired filter in the *Filter* dropdown list. In this example, the Azure Stack SDN connector will automatically populate and update IP addresses only for instances that are

named tfgta:

3. Ensure that the Azure Stack SDN connector resolves dynamic firewall IP addresses:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Hover over the address created in step 2 to see a list of IP addresses for instances that are named tfgta as configured in step 2:



To configure Azure Stack SDN connector using CLI commands:

1. Configure the Azure Stack SDN connector:

```
config system sdn-connector
  edit "azurestack1"
    set type azure
    set azure-region local
    set server "azurestack.external"
    set username "username@azurestoreexamplecompany.onmicrosoft.com"
    set password xxxxx
    set log-in endpoint "https://login.microsoftonline.com/942b80cd-1b14-42a1-8dcf-4b21dece61ba"
    set resource-url
      "https://management.azurestoreexamplecompany.onmicrosoft.com/12b6fedd-9364-4cf0-822b-080d70298323"
    set update-interval 30
  next
end
```

2. Create a dynamic firewall address for the configured Azure Stack SDN connector with the supported Azure Stack filter. In this example, the Azure Stack SDN Connector will automatically populate and update IP addresses only for instances that are named tfgta:

```
config firewall address
  edit "azurestack-address-name1"
    set type dynamic
    set sdn "azurestack1"
```

```

        set filter "vm=tfcta"
    next
end

```

3. Confirm that the Azure Stack fabric connector resolves dynamic firewall IP addresses using the configured filter:

```

config firewall address
    edit "azurestack-address-name1"
        set type dynamic
        set sdn "azurestack1"
        set filter "vm=tfcta"
    config list
        edit "10.0.1.4"
        next
        edit "10.0.2.4"
        next
        edit "10.0.3.4"
        next
        edit "10.0.4.4"
        next
        edit "192.168.102.32"
        next
        edit "192.168.102.35"
        next
    end
next
end

```

Azure SDN connector for non-VM resources

IP address resolving functionality is available for the following Azure resources:

- VM network interfaces (including VMSS)
- Internet-facing load balancers
- Internal load balancers
- Application gateways



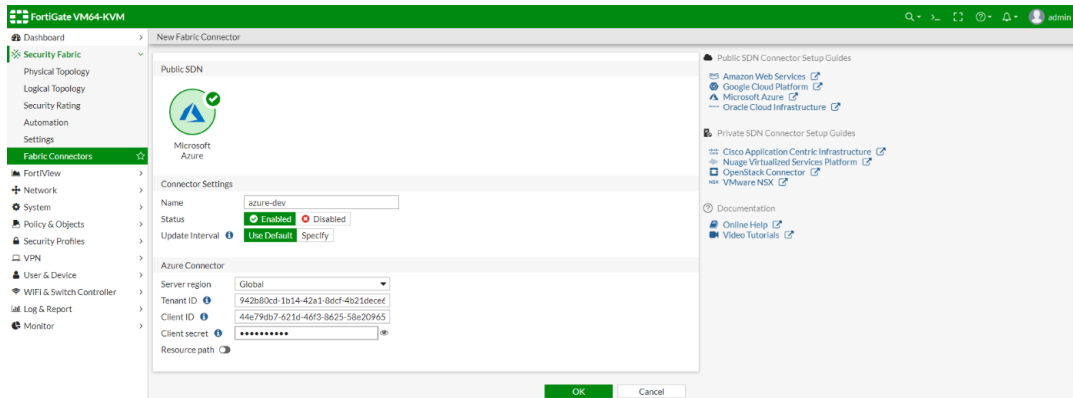
VPN gateways are currently not supported.

The following example demonstrates configuring an internet-facing load balancer.

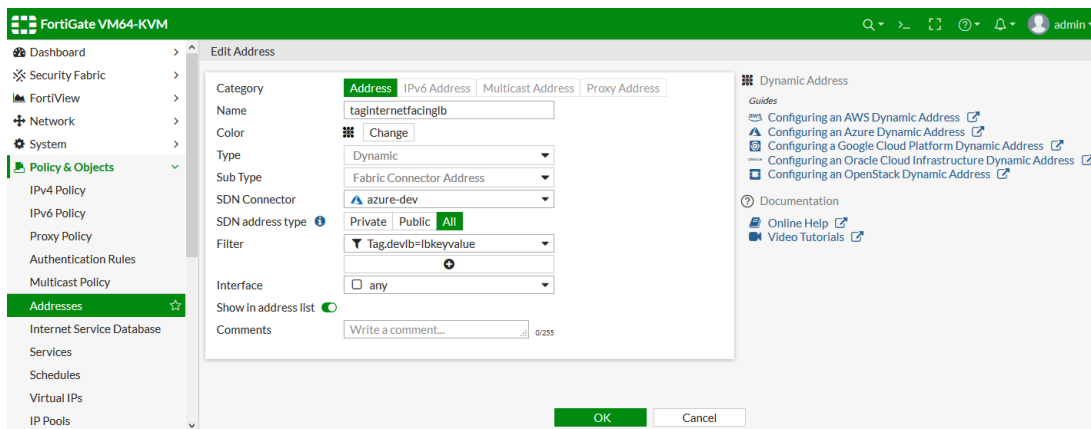
To configure an internet-facing load balancer address in the GUI:

1. Configure the Azure SDN connector:
 - a. Go to *Security Fabric > Fabric Connectors*.
 - b. Click *Create New*, and select *Microsoft Azure*.

- c. Enter the settings based on your deployment, and click **OK**. The update interval is in seconds.



2. Create the dynamic firewall address:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Click *Create New > Address* and enter a name.
 - c. Configure the following settings:
 - i. For *Type*, select *Dynamic*.
 - ii. For *Sub Type*, select *Fabric Connector Address*.
 - iii. For *SDN Connector*, select *azure-dev*.
 - iv. For *SDN address type*, select *All*.
 - v. For *Filter*, enter `Tag.dev1b=1bkeyvalue`.
 - d. Click **OK**.

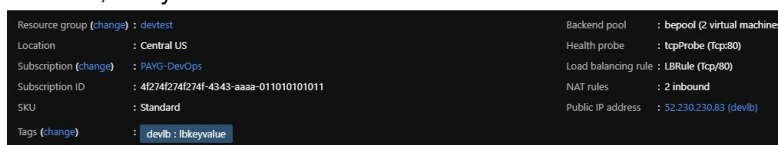


The corresponding IP addresses are dynamically updated and resolved after applying the tag filter.

3. Ensure that the connector resolves the dynamic firewall IP address:
 - a. Go to *Policy & Objects > Addresses*.
 - b. In the address table, hover over the address created in step 2 to view what IP it resolves to:



- c. In Azure, verify to confirm the IP address matches:



To configure an internet-facing load balancer in the CLI:**1. Configure the Azure SDN connector:**

```

config system sdn-connector
  edit "azure-dev"
    set status enable
    set type azure
    set azure-region global
    set tenant-id "942b80cd-1b14-42a1-8dcf-4b21dece61ba"
    set client-id "44e79db7-621d-46f3-8625-58e209654e58"
    set client-secret xxxxxxxxxx
    set update-interval 60
  next
end

```

2. Create the dynamic firewall address:

```

config firewall address
  edit "taginternetfacinglb"
    set type dynamic
    set sdn "azure-dev"
    set filter "Tag.devlb=lbkeyvalue"
    set sdn-addr-type all
  next
end

```

The corresponding IP addresses are dynamically updated and resolved after applying the tag filter.

3. Confirm that the connector resolves the dynamic firewall IP address:

```

config firewall address
  edit "taginternetfacinglb"
    show
    config firewall address
      edit "taginternetfacinglb"
        set uuid df391760-3bb6-51ea-f775-421df18f368d
        set type dynamic
        set sdn "azure-dev"
        set filter "Tag.devlb=lbkeyvalue"
        set sdn-addr-type all
        config list
          edit "52.230.230.83"
          next
        end
      next
    end
  next
end

```

VMware ESXi SDN connector

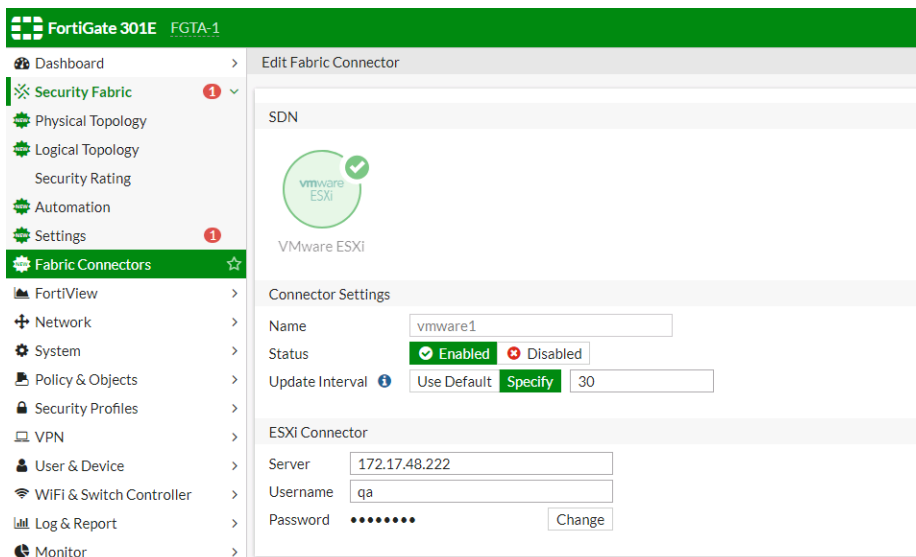
Dynamic addresses for VMware ESXi and vCenter servers can be automatically updated by using a VMware ESXi SDN connector, including mapping the following attributes from VMware ESXi and vCenter objects to dynamic address groups in FortiOS:

- vmid
- host

- name
- uuid
- vmuuid
- vmnetwork
- guestid
- guestname
- annotation

To configure VMware ESXi SDN connector using the GUI:

1. Configure the VMware ESXi SDN connector:
 - a. Go to *Security Fabric > Fabric Connectors*.
 - b. Click *Create New*, and select *VMware ESXi*.
 - c. Configure as shown, substituting the server IP address, username, and password for your deployment. The update interval is in seconds. The password cannot contain single or double quotes.



2. Create a dynamic firewall address for the configured VMware ESXi SDN connector:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Click *Create New*, then select *Address*.
 - c. Configure the address as shown, selecting the desired filter in the *Filter* dropdown list. In this example, the VMware ESXi fabric connector will automatically populate and update IP addresses only for instances that

belong to VLAN80:

3. Ensure that the VMware ESXi SDN connector resolves dynamic firewall IP addresses:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Hover over the address created in step 2 to see a list of IP addresses for instances that belong to VLAN80 as configured in step 2:

Name	Type
Address 2	
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet
SSLVPN_TUNNEL_ADDR1	IP Range
all	Subnet
gmail.com	FQDN
login.microsoft.com	FQDN
login.microsoftonline.com	FQDN
login.windows.net	FQDN
none	
vmware-network	Fabric Connector Address (VMWARE)
Address Group 2	
Wildcard FQDN 2	

vmware-network resolves to:

- 192.168.8.240

To configure VMware ESXi SDN connector using CLI commands:

1. Configure the VMware ESXi SDN connector:

```
config system sdn-connector
edit "vmware1"
set type vmware
set server "172.17.48.222"
set username "example_username"
set password xxxxx
set update-interval 30
next
end
```

2. Create a dynamic firewall address for the configured VMware ESXi SDN connector with the supported VMware ESXi filter. In this example, the VMware ESXi SDN connector will automatically populate and update IP addresses only for instances that belong to the specified VLAN:

```
config firewall address
```

```
edit "vmware-network"
  set type dynamic
  set sdn "vmware1"
  set filter "vmnetwork=VLAN80"
next
end
```

3. Confirm that the VMware ESXi SDN connector resolves dynamic firewall IP addresses using the configured filter:

```
config firewall address
  edit "vmware-network"
    set uuid abfa1748-1b80-51e9-d0fd-ea322b3bba2d
    set type dynamic
    set sdn "vmware1"
    set filter "vmnetwork=VLAN80"
  config list
    edit "192.168.8.240"
    next
  end
next
end
```

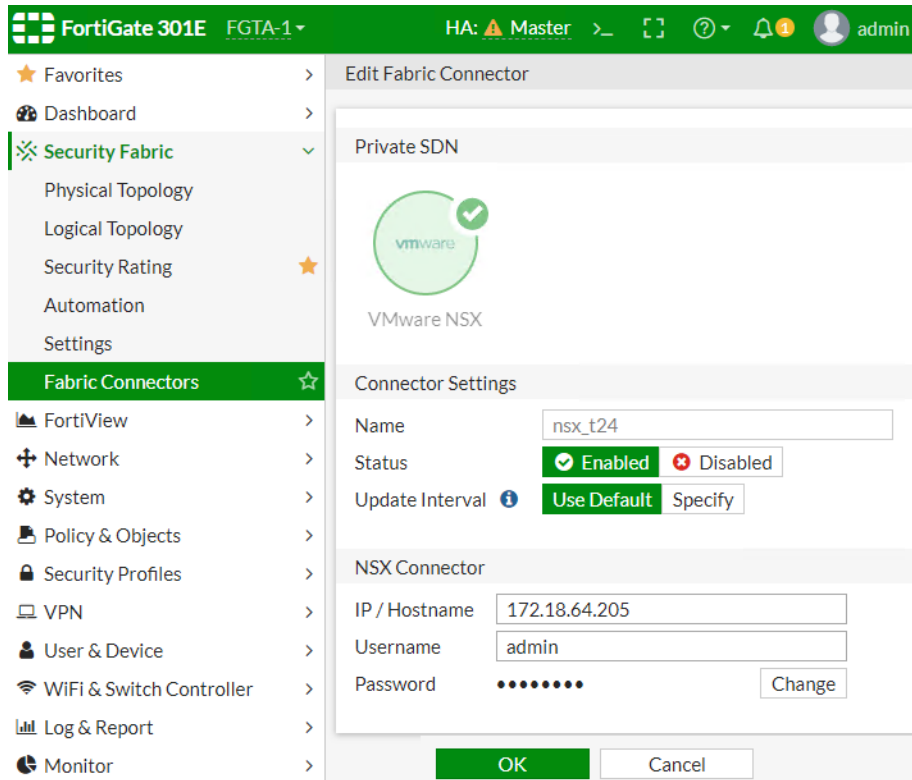
VMware NSX-T manager SDN connector

This feature provides SDN connector configuration for VMware NSX-T manager. You can import specific groups, or all groups from the NSX-T manager.

To configure SDN connector for NSX-T manager in the GUI:

1. Go to *Security Fabric > Fabric Connectors* and click *Create New*.
2. In the *Private SDN* section, click *VMware NSX*.

3. Enter the settings and click OK.

**To configure SDN connector for NSX-T manager in the CLI:**

```
config system sdn-connector
  edit "nsx_t24"
    set type nsx
    set server "172.18.64.205"
    set username "admin"
    set password xxxxxx
  next
end
```

To import a specific group from the NSX-T manager:

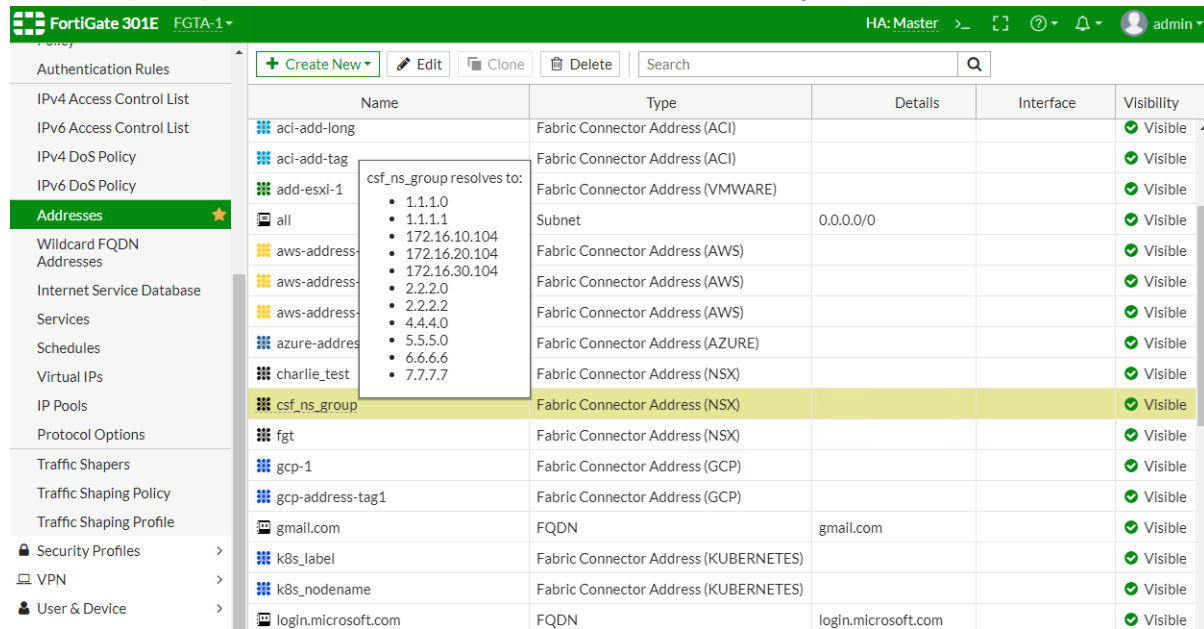
```
# execute nsx group import nsx_t24 root csf_ns_group
[1] 336914ba-0660-4840-b0f1-9320f5c5ca5e csf_ns_group:
Name:csf_ns_group
Address:1.1.1.0
Address:1.1.1.1
Address:172.16.10.104
Address:172.16.20.104
Address:172.16.30.104
Address:2.2.2.0
Address:2.2.2.2
Address:4.4.4.0
Address:5.5.5.0
Address:6.6.6.6
Address:7.7.7.7
```

To import all groups from NSX-T manager:

```
# execute nsx group import nsx_t24 root
[1] 663a7686-b9a3-4659-b06f-b45c908349a0 ServiceInsertion_NSGroup:
    Name:ServiceInsertion_NSGroup
    Address:10.0.0.2
[2] 336914ba-0660-4840-b0f1-9320f5c5ca5e csf_ns_group:
    Name:csf_ns_group
    Address:1.1.1.0
    Address:1.1.1.1
    Address:172.16.10.104
    Address:172.16.20.104
    Address:172.16.30.104
    Address:2.2.2.0
    Address:2.2.2.2
    Address:4.4.4.0
    Address:5.5.5.0
    Address:6.6.6.6
    Address:7.7.7.7
[3] c462ec4d-d526-4ceb-aeb5-3f168cecd89d charlie_test:
    Name:charlie_test
    Address:1.1.1.1
    Address:2.2.2.2
    Address:6.6.6.6
    Address:7.7.7.7
[4] ff4dcb08-53cf-46bd-bef4-f7aeda9c0ad9 fgt:
    Name:fgt
    Address:172.16.10.101
    Address:172.16.10.102
    Address:172.16.20.102
    Address:172.16.30.103
[5] 3dd7df0d-2baa-44e0-b88f-bd21a92eb2e5 yongyu_test:
    Name:yongyu_test
    Address:1.1.1.0
    Address:2.2.2.0
    Address:4.4.4.0
    Address:5.5.5.0
```

To view the dynamic firewall IP addresses that are resolved by the SDN connector in the GUI:

1. Go to *Policy & Objects > Addresses* to view the IP addresses resolved by an SDN connector.



To view the dynamic firewall IP addresses that are resolved by the SDN connector in the CLI:

```
# show firewall address csf_ns_group
config firewall address
  edit "csf_ns_group"
    set uuid ee4a2696-bacd-51e9-f828-59457565b880
    set type dynamic
    set sdn "nsx_t24"
    set obj-id "336914ba-0660-4840-b0f1-9320f5c5ca5e"
    config list
      edit "1.1.1.0"
        next
      edit "1.1.1.1"
        next
      edit "172.16.10.104"
        next
      edit "172.16.20.104"
        next
      edit "172.16.30.104"
        next
      edit "2.2.2.0"
        next
      edit "2.2.2.2"
        next
      edit "4.4.4.0"
        next
      edit "5.5.5.0"
        next
      edit "6.6.6.6"
        next
      edit "7.7.7.7"
```

```

        next
    end
next
end

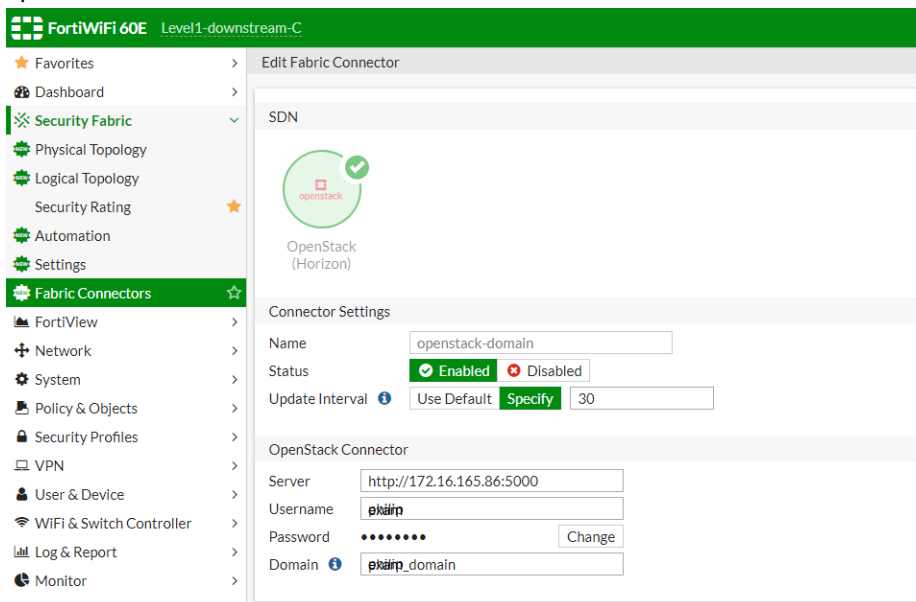
```

OpenStack (Horizon) SDN connector with domain filter

You can select a domain attribute when configuring an OpenStack SDN connector in FortiOS. When a domain is configured for the OpenStack SDN connector, FortiOS resolves OpenStack dynamic firewall addresses from the specified OpenStack domain. If a domain is not specified, FortiOS resolves the dynamic firewall addresses using the default OpenStack domain.

To configure OpenStack SDN connector with a domain filter using the GUI:

1. Configure the OpenStack SDN connector:
 - a. Go to *Security Fabric > Fabric Connectors*.
 - b. Click *Create New*, and select *Openstack (Horizon)*.
 - c. In the *Domain* field, enter the desired domain name from OpenStack. The fabric connector will only resolve IP addresses for instances that belong to the specified domain.
 - d. Configure as shown, substituting the server IP address, username, and password for your deployment. The update interval is in seconds.



2. Create a dynamic firewall address for the configured OpenStack SDN connector:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Click *Create New*, then select *Address*.
 - c. Configure the address as shown, selecting the desired filter in the *Filter* dropdown list. The OpenStack SDN connector will automatically populate and update IP addresses only for instances that belong to the

specified domain and network:

3. Ensure that the OpenStack SDN connector resolves dynamic firewall IP addresses:

- a. Go to **Policy & Objects > Addresses**.
- b. Hover over the address created in step 2 to see a list of IP addresses for instances that belong to the specified domain and specified network as configured in steps 1 and 2:

Name	Type
SSLVPN_TUNNEL_ADDR2	Subnet
all	Subnet
auth.gfx.ms_x2_	FQDN
autoupdate.opera.com	FQDN
azure-vm12	Fabric Connector Address (AZURE)
gmail.com	FQDN
google-play	FQDN
login.microsoft.com	FQDN
login.microsoftonline	FQDN
login.windows.net	FQDN
nsxsecuritygroup1	Address (NSX)
openstack-domain-network	Fabric Connector Address (OPENSTACK)

openstack-domain-network resolves to:

- 10.0.0.13
- 10.0.0.16
- 10.0.0.3
- 172.24.4.18
- 172.24.4.24
- 172.24.4.3

To configure OpenStack SDN connector with a domain filter using CLI commands:

1. Configure the OpenStack SDN connector. The SDN connector will only resolve IP addresses for instances that belong to the specified domain:

```
config system sdn-connector
  edit "openstack-domain"
    set type openstack
    set server "http://172.16.165.86:5000"
    set username "example_username"
    set password xxxxxx
    set domain "example_domain"
    set update-interval 30
  next
end
```

2. Create a dynamic firewall address for the configured OpenStack SDN connector with the supported OpenStack filter. The OpenStack SDN connector will automatically populate and update IP addresses only for instances that belong to the specified domain and the specified network:

```
config firewall address
  edit "openstack-domain-network"
    set type dynamic
    set sdn "openstack-domain"
    set filter "Network=example-net1"
  next
end
```

3. Confirm that the OpenStack SDN connector resolves dynamic firewall IP addresses using the configured domain and filter:

```
config firewall address
  edit "openstack-domain-network"
    set uuid 02837298-234d-51e9-efda-559c6001438a
    set type dynamic
    set sdn "openstack-domain"
    set filter "Network=example-net1"
  config list
    edit "10.0.0.13"
    next
    edit "10.0.0.16"
    next
    edit "10.0.0.3"
    next
    edit "172.24.4.18"
    next
    edit "172.24.4.24"
    next
    edit "172.24.4.3"
    next
  end
next
end
```

OCI SDN connector

You can configure Security Fabric connector integration with Oracle Cloud Infrastructure (OCI).

To configure an OCI SDN connector in the CLI:

1. Configure an SDN connector:

```
config system sdn-connector
  edit "ocil"
    set status enable
    set type oci
    set tenant-id
    "ocidl.tenancy.oc1..aaaaaaaa3aaaaaaaaaaaaaaaaa77xxxxx54bbbbbb4xxxx35xx55xxxx"
    set user-id
    "ocidl.user.oc1..aaaaaaaa2laaaaa3aaaaaaaaabbbbbbbbbbcccc3ccccccccccccccccxxxx"
    set compartment-id
    "ocidl.compartment.oc1..aaaaaaaaaaaaaaaa7bbbbbbbbbcccccccccc6xxx53xxxx7xxxxxxxxxx"
    set oci-region "us-ashburn-1"
```



```

        set oci-region-type commercial
        set oci-cert "cert-sha2"
        set update-interval 30
    next
end

```

2. Create a dynamic firewall address for the SDN connector with a supported filter:

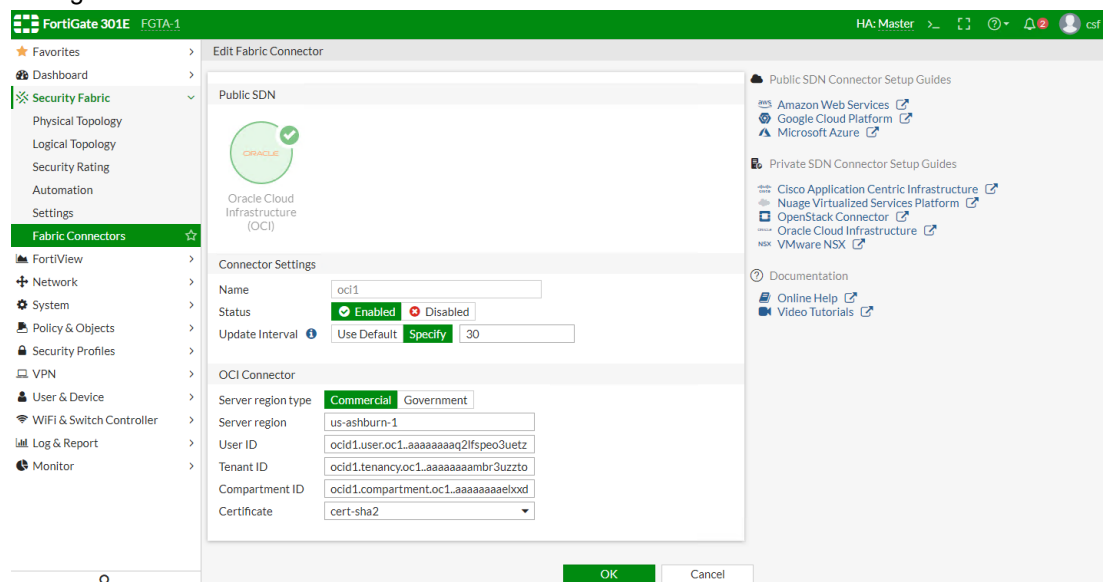
```

config firewall address
    edit "oci-address-1"
        set uuid 0b4a496e-8974-51e9-e223-fee75c935fb7
        set type dynamic
        set sdn "oci1"
        set filter "CompartmentName=DevelopmentEngineering"
    next
end

```

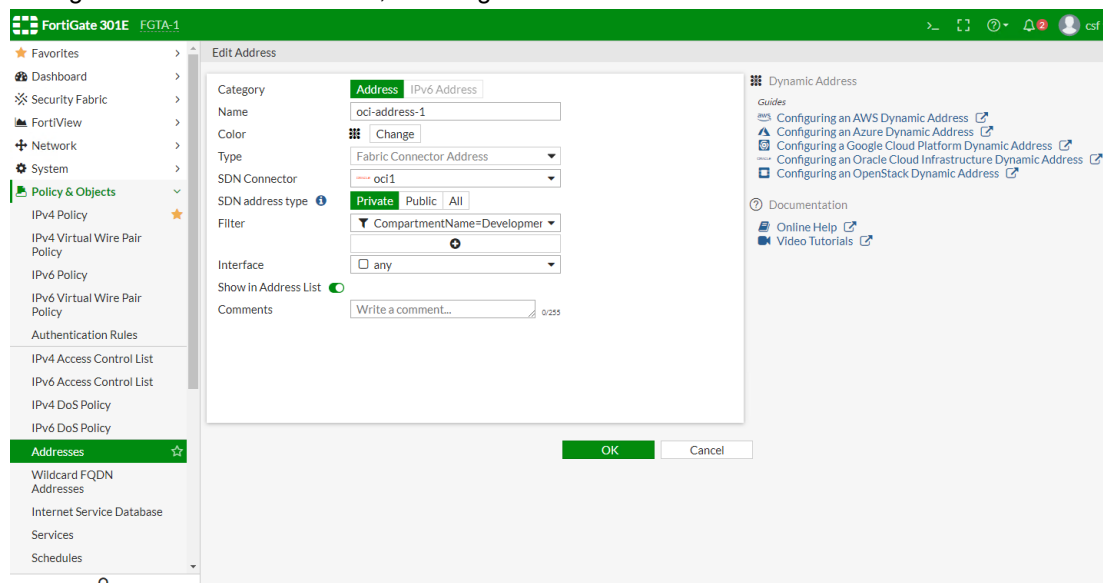
To configure an OCI SDN connector in the GUI:

1. Go to *Security Fabric > Fabric Connectors* and click *Create New*.
2. In the *Public SDN* section, select *Oracle Cloud Infrastructure (OCI)*.
3. Configuration the connector as needed.



4. Click *OK*.
5. Go to *Policy & Objects > Addresses* and click *Create New > Address*.

6. Configure the address as needed, selecting the OCI connector in the *SDN Connector* field.



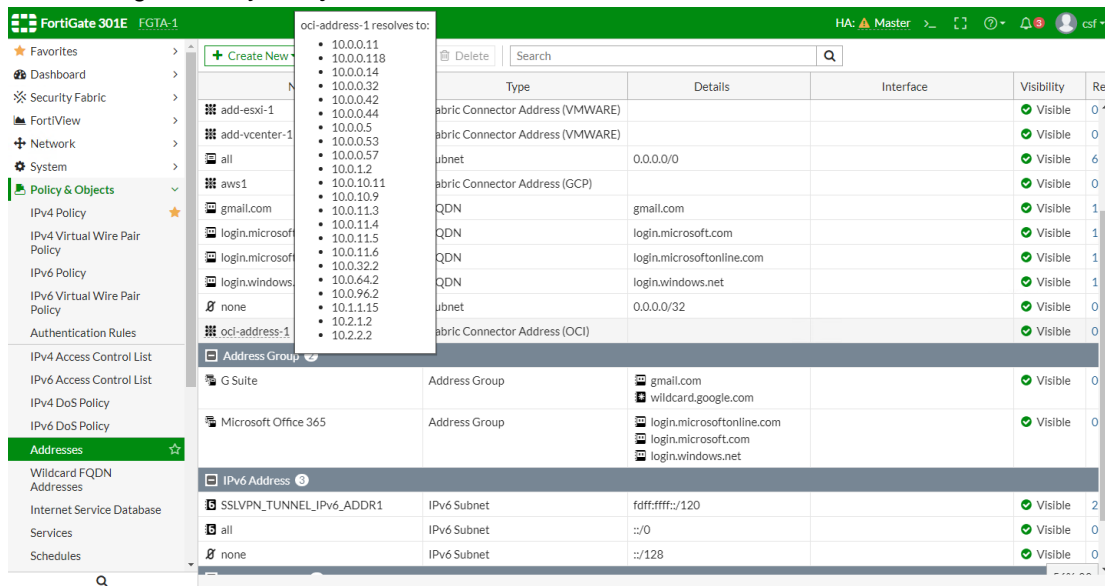
7. Click OK.

To confirm that dynamic firewall addresses are resolved by the SDN connector:

1. In the CLI, check that the addresses are listed:

```
config firewall address
  edit "oci-address-1"
    set uuid 0b4a496e-8974-51e9-e223-fee75c935fb7
    set type dynamic
    set sdn "oci1"
    set filter "CompartmentName=DevelopmentEngineering"
  config list
    edit "10.0.0.11"
    next
    edit "10.0.0.118"
    next
    ...
  next
end
next
end
```

2. In the GUI, go to **Policy & Objects > Addresses** and hover the cursor over the address name.



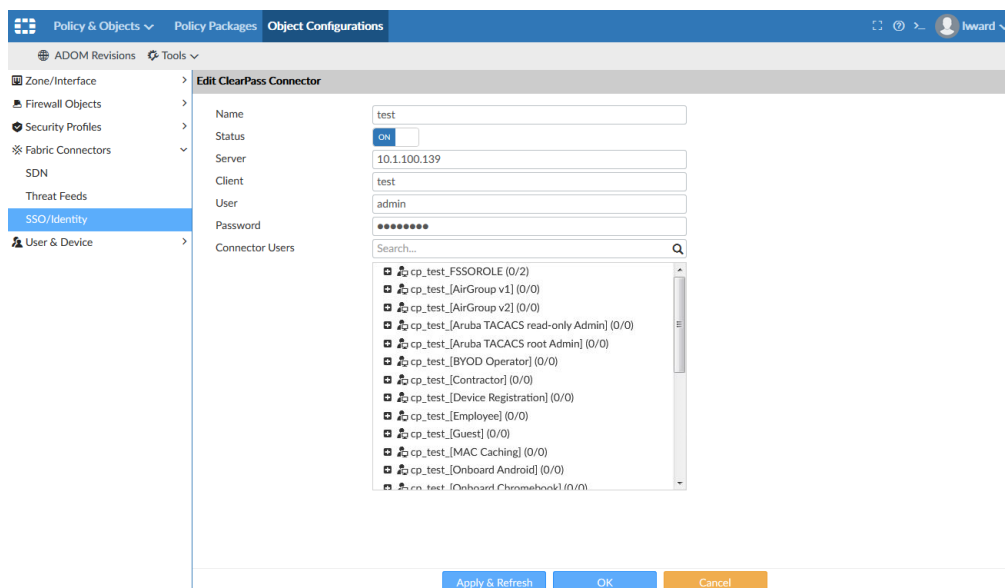
ClearPass endpoint connector via FortiManager

ClearPass Policy Manager (CPPM) is a network access system that can send information about authenticated users to third party systems, such as a FortiGate or FortiManager.

In this example, communications are established between CPPM and FortiManager, and then the FortiManager forwards information to a managed FortiGate. On the FortiGate, the user information can be used in firewall policies and added to FSSO dynamic addresses.

Configure the FortiManager

Establish communications between FortiManager and CPPM so that FortiManager can synchronize CPPM user groups. See [Creating a ClearPass connector](#) in the FortiManager Administration Guide.

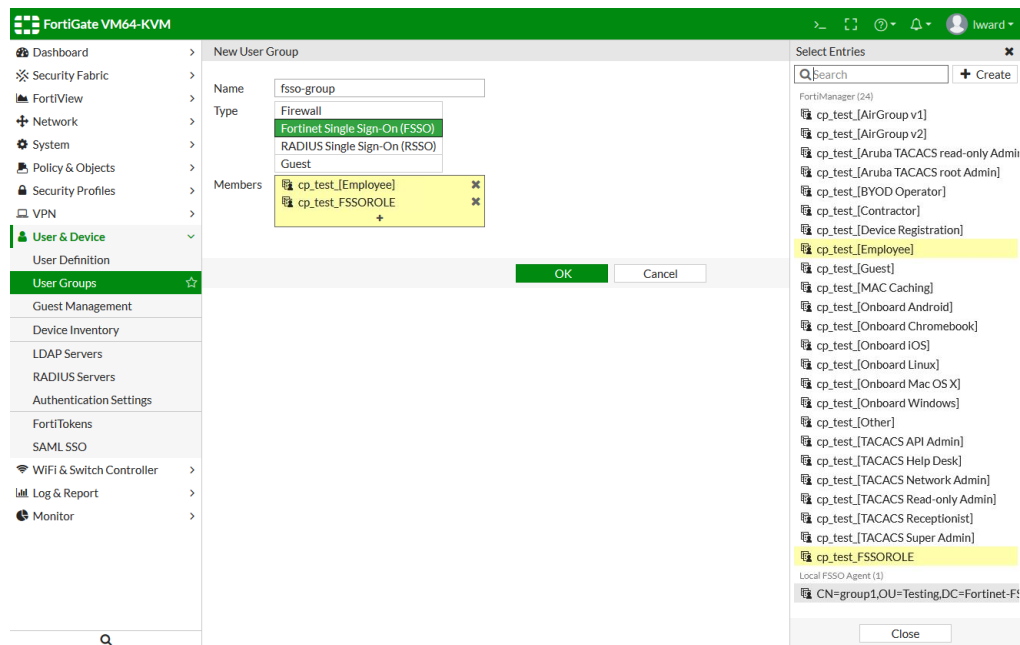


FortiManager forwards the group information to managed FortiGates.

Add CPPM FSSO user groups to a local user group

To add CPPM user groups to a local user group in the GUI:

1. On the FortiGate, go to *User & Device > User Groups*.
2. Click *Create New*.
3. Enter a name for the group and set *Type* to *Fortinet Single Sign-On (FSSO)*.
4. Click the *Members* field, and add one or more FSSO groups.
FSSO groups can come from multiple sources; CPPM FSSO groups are prefixed with *cp_* and are listed under the *FortiManager* heading.



5. Click *OK*.

To add CPPM user groups to a local user group in the CLI:

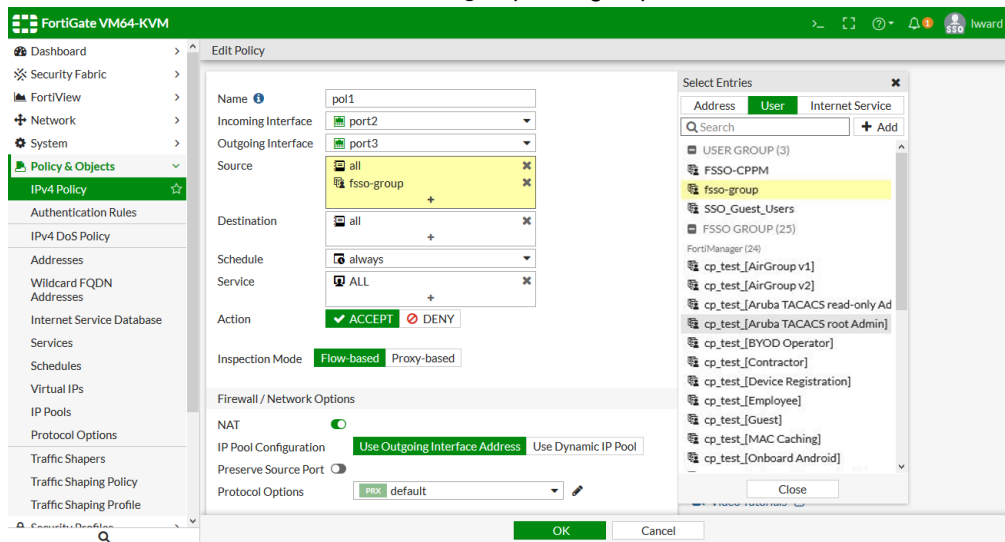
```
config user group
  edit fssso-group
    set group-type fssso-service
    set member "cp_test_[Employee]" "cp_test_FSSOROLE"
  next
end
```

Use the local FSSO user group in a firewall policy

To add the local FSSO user group to a firewall policy in the GUI:

1. Go to *Policy & Objects > IPv4 Policy*.
2. Create a new policy, or edit an existing one.

- Click in the *Source* field and add the *fsso-group* user group.



CPPM user groups can also be added directly to the policy.

- Click OK.

To add the local FSSO user group to a firewall policy in the CLI:

```
config firewall policy
  edit 1
    set name "pol1"
    set uuid 2b88ed8a-c906-51e9-fb25-8cb12172acd8
    set srcintf "port2"
    set dstintf "port3"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set logtraffic all
    set groups "fsso-group"
    set nat enable
  next
end
```

Verification

To verify that a user was added to the FSSO list on the FortiGate:

- Log on to the client and authenticate with CPPM.
After successful authentication, the user is added to the FSSO list on the FortiGate.

- On the FortiGate, go to *Monitor > Firewall User Monitor* to verify that the user was added.

User Name	User Group	Duration	IP Address	Traffic Volume	Method
fsso2	fsso-group	9 second(s)	10.1.100.188	0 B	Fortinet Single Sign-On
	cp_test_FSSOROLE				

The user group `cp_test_FSSOROLE` is listed separately because the user is a member of that group on the CPPM.

To verify that traffic can pass the firewall:

- Log on to the client and browse to an external website.
- On the FortiGate, go to *FortiView > Sources*.
- Double-click on the user and select the *Destinations* tab to verify that traffic is being passed by the firewall.

To verify the user address groups:

```
show user adgrp
config user adgrp
    edit "cp_test_FSSOROLE"
        set server-name "FortiManager"
    next
    edit "cp_test_[AirGroup v1]"
        set server-name "FortiManager"
    next
    edit "cp_test_[AirGroup v2]"
        set server-name "FortiManager"
    next
    edit "cp_test_[Aruba TACACS read-only Admin]"
        set server-name "FortiManager"
    next
    edit "cp_test_[Aruba TACACS root Admin]"
        set server-name "FortiManager"
    next
    edit "cp_test_[BYOD Operator]"
        set server-name "FortiManager"
    next
    edit "cp_test_[Contractor]"
        set server-name "FortiManager"
    next
    edit "cp_test_[Device Registration]"
        set server-name "FortiManager"
    next
    ...
```

```

edit "CN=group1,OU=Testing,DC=Fortinet-FSSO,DC=COM"
    set server-name "Local FSSO Agent"    <----- !!!
next
end

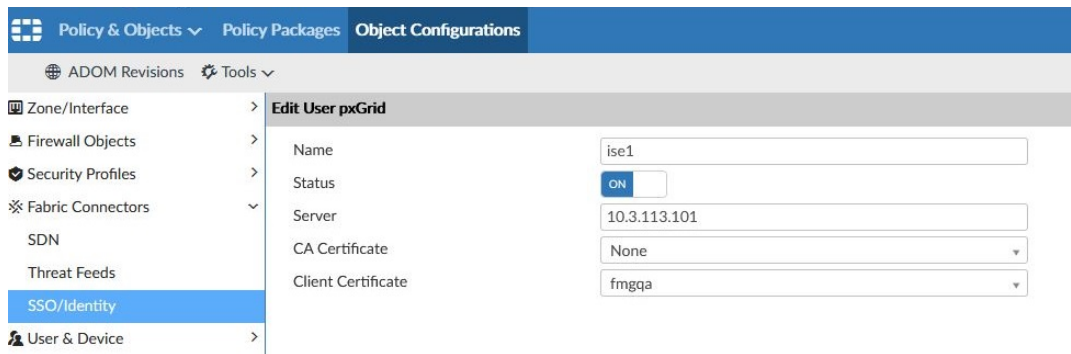
```

Cisco pxGrid fabric connector

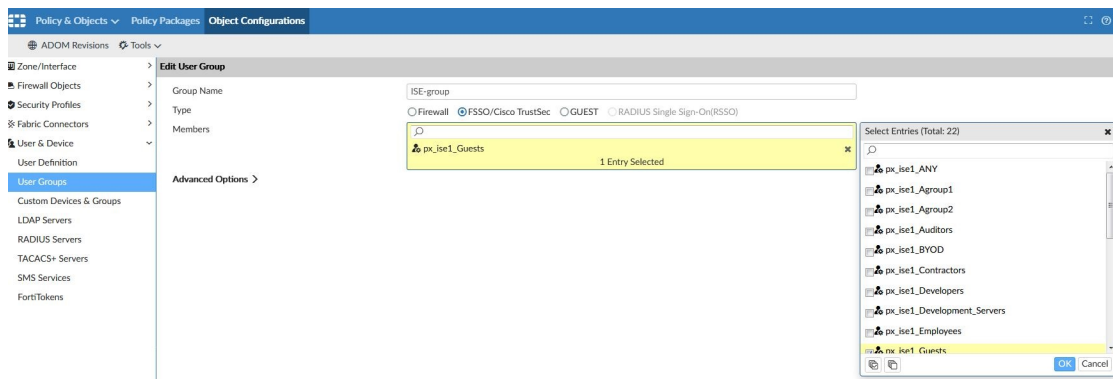
You can create an endpoint connector to Cisco pxGrid by using FortiManager. FortiManager dynamically collects updates from pxGrid and forwards them to FortiGate by using the Fortinet Single Sign On (FSSO) protocol.

To create a Cisco pxGrid fabric connector:

1. On FortiManager, create an SSO Connector to Cisco ISE.
Communication between FortiManager and Cisco ISE is secured by using TLS. FortiManager requires a client certificate issued by Cisco ISE. FortiManager uses the certificate to authenticate to Cisco ISE.



2. On FortiManager, map Cisco ISE groups to a Fortinet FSSO group.
Once a secured communication channel is established, Cisco sends all user groups to FortiManager. The FortiManager administrator can select specific groups and map them to Fortinet FSSO groups.



3. On FortiManager, add Fortinet FSSO group to a firewall policy in a policy package.

The screenshot shows the FortiManager interface for editing a policy package. The left sidebar shows the tree structure: Policy Packages > Object Configurations > default > IPv4 Policy > Installation Targets. The main area is titled 'Edit IPv4 Policy'. The configuration fields are as follows:

- Name: (empty)
- Incoming Interface: any
- Outgoing Interface: any
- Source Internet Service: OFF
- Source Address: all
- Source User: +
- Source User Group: ISE-group
- FSSO: ☒
- RSSO: ☐
- Destination Internet Service: OFF
- Destination Address: all
- Service: ALL
- Schedule: always
- Action: Deny, Accept, IPSEC (Accept is selected)
- Log Traffic: ☐ No Log, ☒ Log Security Events, ☐ Log All Sessions
- ☐ Generate Logs when Session Starts
- ☐ Capture Packets
- NAT: ☐
- Security Profiles: ☐
- Shared Shaper: +
- Reverse Shaper: +
- Per-IP Shaper: +
- Comments: 0/1023

Buttons at the bottom: OK, Cancel.

4. On FortiManager, synchronize the policy package to the firewall for the managed FortiGate.

The screenshot shows the FortiManager Device Manager interface. The top bar shows 'Device Manager' and 'Device & Groups'. The main area shows a table of devices with columns: Device Name, Config Status, Policy Package Status, CLI Template Status, and Firmware Version. The table has one entry: FortiGate-400D, which is 'Synchronized' and has a 'default' policy package. A dialog box titled 'Install Wizard - Policy Package (default)' is open, showing the progress of the installation. The wizard has two steps: 1. FortiGate-400D[copy] - root (Copy to device done) and 2. Write summary[preview] (Write preview done). Below the steps, there are green checkmarks for 'Interface Validation', 'Policy and Object Validation', and 'Ready to Install'. At the bottom, there is a table with columns: Device Name, Status, and Action. The table has one entry: FortiGate-400D[root] with a status of 'Connection Up' and actions 'Install Preview' and 'Policy Package Diff'. Buttons at the bottom: Install, Cancel.

5. On FortiGate, verify that the synced firewall policy contains the correct FSSO group and that all FSSO-related information in user `adgrp` is correct.

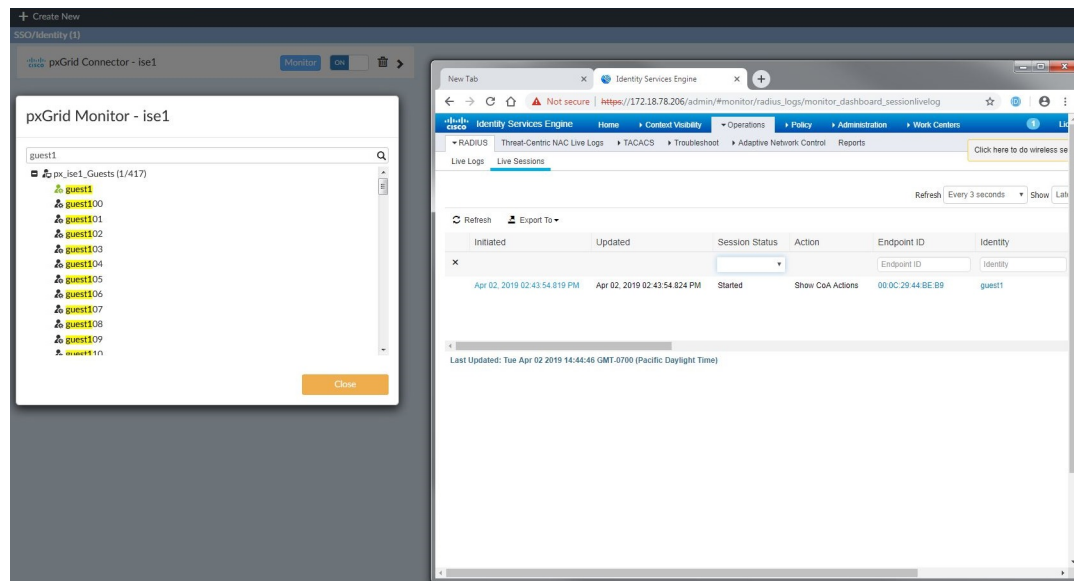

```

config firewall policy
edit 1
set uuid b803052e-562a-51e9-0561-82525c8bcaa9
set srcintf "any"
set dstintf "any"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set groups "ISE-group"
next
end

FortiGate-400D # show user adgrp
config user adgrp
edit "px_isel_ANY"
set server-name "FortiManager"
next
edit "px_isel_Agroup1"
set server-name "FortiManager"
next
edit "px_isel_Agroup2"
set server-name "FortiManager"
next
edit "px_isel_Auditors"
set server-name "FortiManager"
next
edit "px_isel_BYOD"
set server-name "FortiManager"
next
edit "px_isel_Contractors"
set server-name "FortiManager"
next
edit "px_isel_Developers"
set server-name "FortiManager"
next
edit "px_isel_Development_Servers"
set server-name "FortiManager"
next
edit "px_isel_Employees"
set server-name "FortiManager"
next
edit "px_isel_Guests"
set server-name "FortiManager"
next
edit "px_isel_HR"
set server-name "FortiManager"
next
edit "px_isel_Network_Services"
set server-name "FortiManager"

```

6. After successful user authentication on Cisco ISE, verify that information is forwarded to FortiManager. On FortiManager, the icon next to the authenticated user in *pxGrid Monitor* should be green.



FortiGate should have two entries: one in the firewall-authenticated user list and one in the FSSO logged-on user list.

In the FSSO logged-on user list, you can view both groups. You view the group that the user belongs to on Cisco ISE and the Fortinet FSSO group.

```

FortiGate-400D #
FortiGate-400D # dia deb authd fso 1
-----FSSO logons-----
IP: 10.1.100.188  User: guest1  Groups: px_isel_Guests  Workstation:  MemberOf: ISE-group
Total number of logons listed: 1, filtered: 0
-----end of FSSO logons-----
FortiGate-400D # dia firewall auth 1
10.1.100.188, guest1
  type: fso, id: 0, duration: S969#, idled: S969#
  server: FortiManager
  packets: in 0 out 0, bytes: in 0 out 0
  group_id: 2
  group_name: ISE-group
----- 1 listed, 0 filtered -----

```

Cisco ACI SDN connector

You can use Cisco ACI (Application Centric Infrastructure) SDN connectors in dynamic firewall addresses.

The Fortinet SDN Connector for Cisco ACI and Nuage Networks is a standalone connector that connects to SDN controllers within Cisco ACI and Nuage Networks. You must configure a connection to the Fortinet SDN connector in FortiOS to query the dynamic addresses.

To configure a Cisco ACI connector in the GUI:

1. Create the Cisco ACI SDN connector:
 - a. Go to *Security Fabric > Fabric Connectors* and click *Create New*.
 - b. In the *Private SDN* section, click *Application Centric Infrastructure (ACI)*.
 - c. Configure the settings as needed.
 - d. Click *OK*.

New External Connector

Private SDN

Application Centric Infrastructure (ACI)

Connector Settings

Name: aci1

Status: Enabled Disabled

Cisco ACI Connector

IP: 172.18.64.31

Port: Use Default Specify

Username: admin

Password: *****

OK Cancel

Public SDN Connector Setup Guides

- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure
- Oracle Cloud Infrastructure

Private SDN Connector Setup Guides

- Cisco Application Centric Infrastructure
- Nuage Virtualized Services Platform
- OpenStack Connector
- VMware NSX

Documentation

- Online Help
- Video Tutorials

2. Create the dynamic firewall address for the connector:
 - a. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
 - b. Configure the following settings:
 - i. For *Type*, select *Dynamic*.
 - ii. For *Sub Type*, select *Fabric Connector Address*.
 - iii. For *SDN Connector*, select the first ACI connector.
 - iv. Configure the remaining settings as needed.

c. Click OK.

To verify the dynamic firewall IPs are resolved by the SDN connector in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. In the address table, hover over the address to view which IPs it resolves to.

To configure a Cisco ACI connector in the CLI:

1. Create the SDN connector:

```
config system sdn-connector
  edit "aci1"
    set type aci
    set server "172.18.64.31"
    set username "admin"
    set password xxxxxxxx
  next
end
```

2. Create the dynamic firewall address for the connector:

```
config firewall address
  edit "aci-address1"
    set type dynamic
    set sdn "aci1"
    set color 17
    set tenant "wqdai-ten"
    set epd-name "EPG-in"
    set sdn-tag "fffff"
  next
end
```

To verify the dynamic firewall IPs are resolved by the SDN connector in the CLI:

```
# diagnose firewall dynamic list

List all dynamic addresses:
aci1.aci.wqdai-ten.EPG-in.fffff: ID(171)
  ADDR(192.168.100.20)
```

Nuage SDN connector

Nuage SDN connectors can be used in dynamic firewall addresses.

The Fortinet SDN Connector for Cisco ACI and Nuage Networks is a standalone connector that connects to SDN controllers within Cisco ACI and Nuage Networks. You must configure a connection to the Fortinet SDN connector in FortiOS to query the dynamic addresses.

To configure a Nuage connector in the GUI:

1. Create the Nuage SDN connector:
 - a. Go to *Security Fabric > Fabric Connectors* and click *Create New*.
 - b. In the *Private SDN* section, click *Nuage Virtualized Services Platform*.
 - c. Configure the settings as needed.
 - d. Click *OK*.

2. Create the dynamic firewall address for the connector:
 - a. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
 - b. Configure the following settings:
 - i. For *Type*, select *Dynamic*.
 - ii. For *Sub Type*, select *Fabric Connector Address*.
 - iii. For *SDN Connector*, select the first the first Nuage connector.
 - iv. Configure the remaining settings as needed.
 - c. Click *OK*.

To verify the SDN connector resolves the dynamic firewall IP addresses in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. In the address table, hover over an address to view which IP addresses it resolves to.

To configure a Nuage connector in the CLI:**1. Create the SDN connector:**

```
config system sdn-connector
  edit "nuage1"
    set type nuage
    set server "172.18.64.27"
    set server-port 5671
    set username "admin"
    set password xxxxxxxx
  next
end
```

2. Create the dynamic firewall address for the connector:

```
config firewall address
  edit "nuage-address1"
    set type dynamic
    set sdn "nuage1"
    set color 19
    set organization "nuage/L3"
    set subnet-name "Subnet20"
  next
end
```

To verify the SDN connector resolves the dynamic firewall IP addresses in the CLI:

```
# diagnose firewall dynamic list
```

List all dynamic addresses:

```
nuage1.nuage.nuage/L3.Subnet20.*: ID(196)
  ADDR(192.168.20.92)
  ADDR(192.168.20.240)
```

Multiple concurrent SDN connectors

You can configure multiple instances for every SDN connector. The specific connector instance must be specified when creating a dynamic firewall address.

This topic provides examples of how to create two Microsoft Azure SDN connectors and use them in new dynamic firewall addresses.



Multiple concurrent SDN/Cloud connectors are not supported yet for Cisco ACI or Nuage.

To create and use two new SDN connectors with the CLI:**1. Create two new SDN connectors:**

```
config system sdn-connector
  edit "azure1"
    set type azure
```

```

        set tenant-id "942b80cd-bbbb-42a1-8888-4b21dece61ba"
        set subscription-id "2f96c44c-cccc-4621-bbbb-65ba45185e0c"
        set client-id "14dbd5cc-3333-4ea4-8888-68738141feb1"
        set client-secret xxxxx
        set update-interval 30
    next
    edit "azure2"
        set type azure
        set tenant-id "942b80cd-bbbb-42a1-8888-4b21dece61ba"
        set client-id "3baa0acc-ffff-4444-b292-0777a2c36be6"
        set client-secret xxxxx
        set update-interval 30
    next
end

```

2. Create new dynamic firewall addresses that use the new connectors:

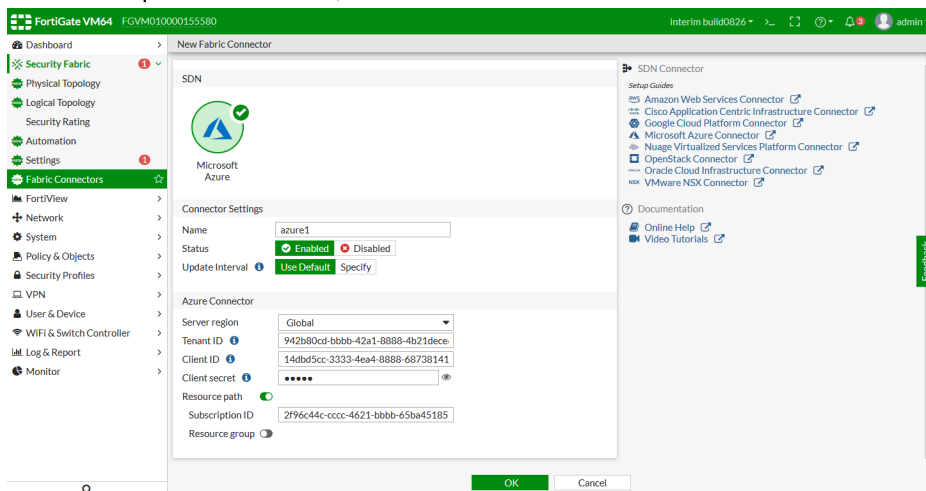
```

config firewall address
    edit "azure-address-location1"
        set type dynamic
        set color 2
        set sdn azure1
        set filter "location=WestUs"
    next
    edit "azure-address-location2"
        set type dynamic
        set color 2
        set sdn azure2
        set filter "location=NorthEurope"
    next
end

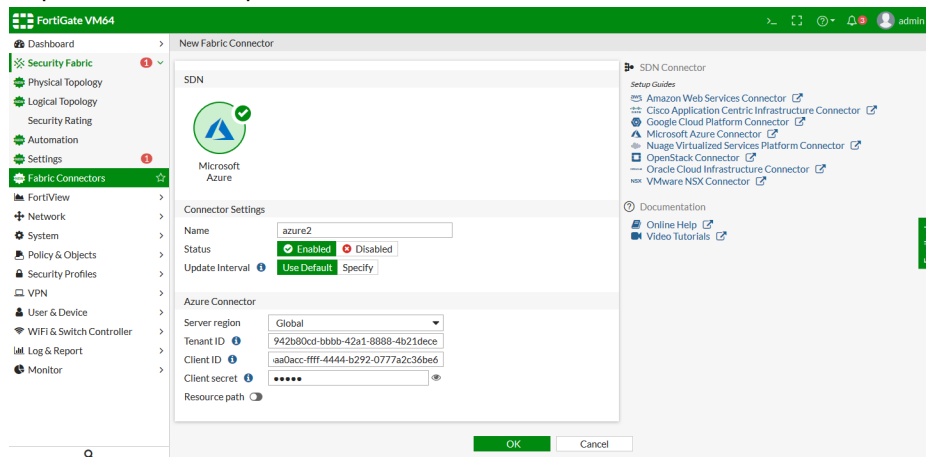
```

To create and use two new SDN connectors with the GUI:

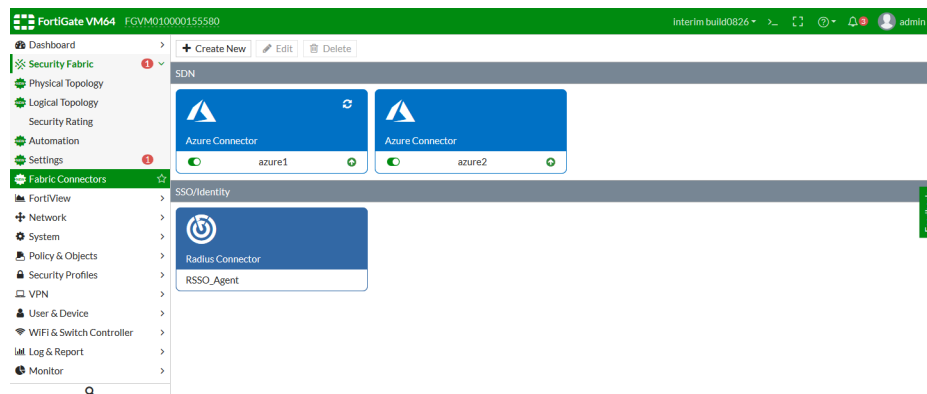
1. Create two new SDN connectors:
 - a. Go to *Security Fabric > Fabric Connectors*, and click *Create New* in the toolbar.
 - b. Click on *Microsoft Azure*.
 - c. Fill in the required information, then click *OK*.



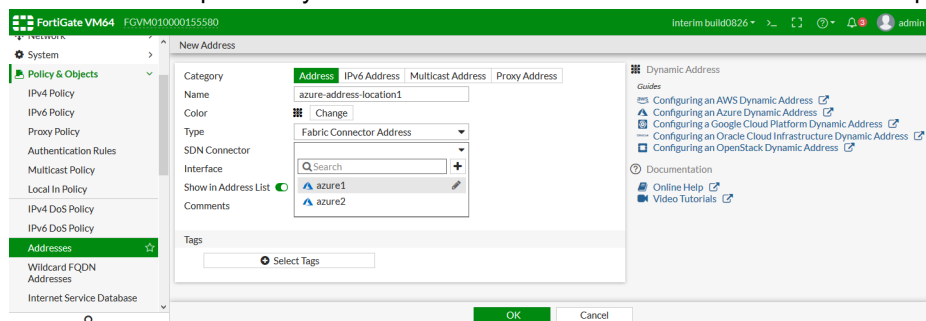
- d. Repeat the above steps for the second connector.



Two Microsoft Azure connectors will now be created.



2. Create new dynamic firewall addresses that use the new connectors:
 - a. Go to **Policy and Objects > Addresses** and click **Create New > Address** in the toolbar.
 - b. Enter a name for the address, and select **Fabric Connector Address** for the **Type**.
 - c. Select one of the previously created SDN connectors from the **SDN Connector** drop down list.



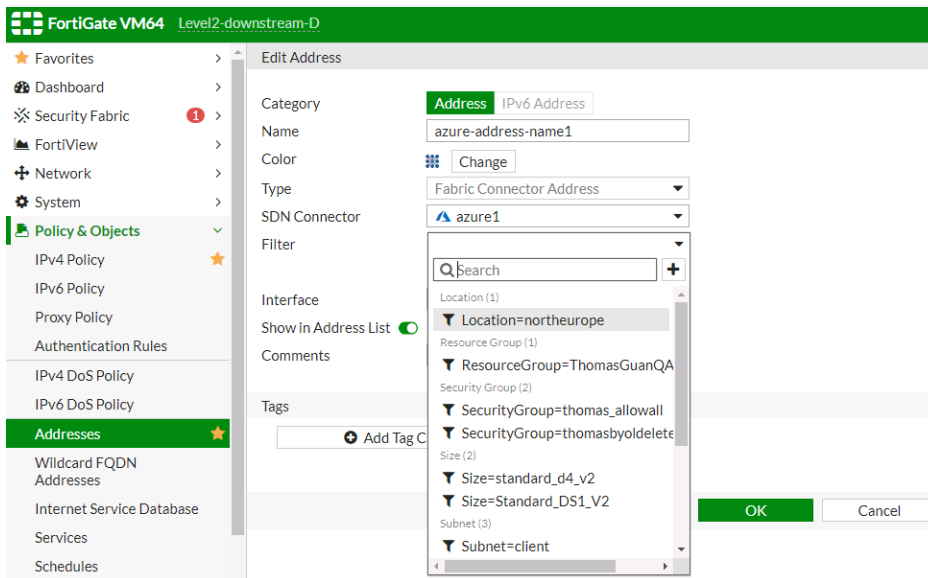
- d. Configure the rest of the required information, then click **OK** to create the address.
- e. Repeat the above steps to create the second address, selecting the other Microsoft Azure SDN connector.

Filter lookup in SDN connectors

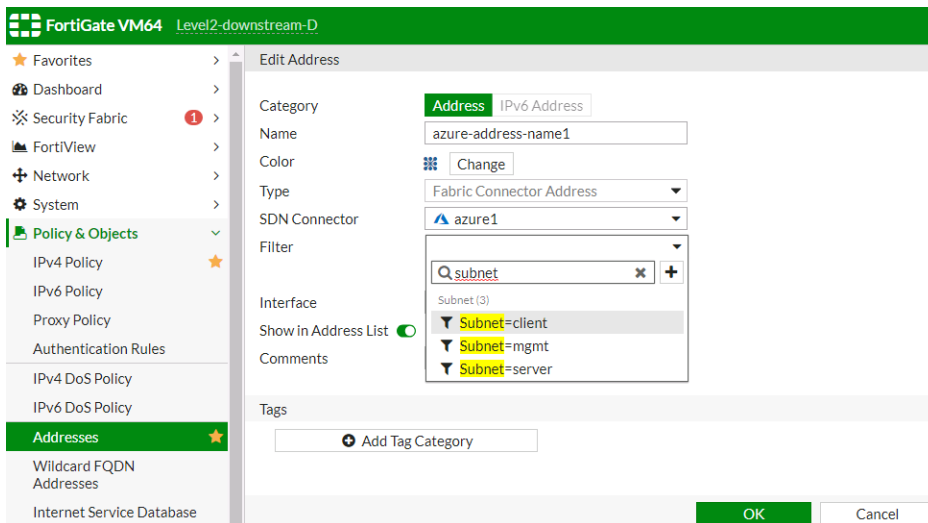
When configuring dynamic address mappings for filters in SDN connectors for Azure, GCP, OpenStack, Kubernetes, and AliCloud, FortiGate can query the filters automatically.

To use the filter lookup:

1. Navigate to *Policy & Objects > Addresses*.
2. Create or edit an SDN connector type dynamic IP address.
Supported SDN connector types include: AWS, Azure, GCP, OpenStack, Kubernetes, and AliCloud. The example below is for an Azure SDN connector.
3. In the address *Filter* field, you can perform the following actions:
 - List all available filters.



- Search the available filters.



- Create custom filters.

The first screenshot shows the 'Edit Address' configuration page for an IPv6 address named 'azure-address-name1'. The 'Filter' dropdown menu is open, displaying a search bar and a list of filters including 'Location=northeurope', 'ResourceGroup=thomasGuanQA', 'SecurityGroup=thomas_allowall', 'SecurityGroup=thomasbydelete', 'Size=standard_d4_v2', 'Size=Standard_DS1_V2', and 'Subnet=client'. The 'OK' and 'Cancel' buttons are visible at the bottom right.

The second screenshot shows the 'New Filter' configuration page. The 'Filter' text box contains the value 'Vm=webserver'. The 'OK' button is visible at the bottom right.

The third screenshot shows the 'Edit Address' configuration page again, with the 'Filter' dropdown menu open. The list of filters now includes 'Vm=webserver' (highlighted in orange), along with other filters like 'Vm=fortiosbyol0228', 'Vm=thomasqa-ubuntu-client', 'Vm=thomasqa-ubuntu-server', and 'Vnet=thomasqa_azure'. The 'OK' and 'Cancel' buttons are visible at the bottom right.

- Set filter logic [and|or].

FortiGate VM64 Level2-downstream-D

★ Favorites

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

IPv4 Policy

IPv6 Policy

Proxy Policy

Authentication Rules

IPv4 DoS Policy

IPv6 DoS Policy

Addresses

Wildcard FQDN

Addresses

Internet Service Database

Services

Schedules

Edit Address

Category: Address IPv6 Address

Name: azure-address-name1

Color: Change

Type: Fabric Connector Address

SDN Connector: azure1

Filter: Location=northeurope, ResourceGroup=ThomasGuanQA, Subnet=server

Interface: any

Show in Address List: ☒

Comments: 0/255

Tags: Add Tag Category

OK Cancel

Support for wildcard SDN connectors in filter configurations

Wildcards are supported for SDN connectors when configuring dynamic address filters.

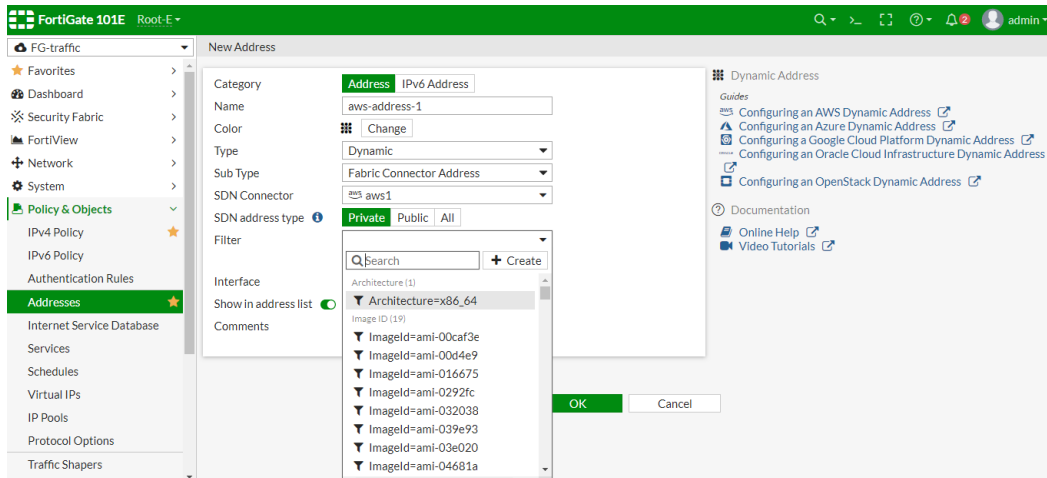
The following SDN connector types are currently supported:

- AWS
- Azure
- Google Cloud Platform
- Kubernetes
- OpenStack
- Oracle Cloud Infrastructure
- VMware ESXi

To configure a dynamic address filter for AWS in the GUI:

1. Create the SDN connector:
 - a. Go to *Security Fabric > Fabric Connectors*.
 - b. Click *Create New*.
 - c. In the *Public SDN* section, click *Amazon Web Services (AWS)*.
 - d. Configure the settings as needed.
 - e. Click *OK*.
2. Create the dynamic firewall address:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Click *Create New > Address*
 - c. Enter a name for the address, then configure the following settings:
 - Set *Type* to *Dynamic*.
 - Set *Sub Type* to *Fabric Connector Address*.
 - Set *SDN Connector* to *aws1*.

- Set *SDN address type* to *Private*.
- For *Filter*, click *Create*, enter `Tag.Name=aws*`, then click *OK*.



d. Click *OK*.

3. In the address table, hover over the address to view what IPs it resolves to.

Name	Type	Details	Interface	Visibility
FIREWALL_A	aws-address-1 resolves to:	18.234.167.123 3.81.41.167 52.87.157.127	ipbnet	0.0.0.0/0
SSLVPN_TUN	Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.FG-traffic)	Visible
all	ipbnet	0.0.0.0/0		Visible
aws-address-1	Dynamic (AWS)			Visible

4. In AWS, verify to confirm the IP addresses match.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	IPv4 Public IP	Key Name
aws_ond	i-023b73b73b73b3b7	t2.micro	us-east-1b	running	2/2 checks ...	18.234.167.123	thomaskeypair
aws_ond	i-04c34c34c34c4c4c3	t2.small	us-east-1d	running	2/2 checks ...	3.81.41.167	thomaskeypair
awsondemand	i-0e0a70a70a70a70a7	t2.micro	us-east-1b	running	2/2 checks ...	52.87.157.127	thomaskeypair

To configure a dynamic address filter for AWS in the CLI:

1. Configure the SDN connector:

```
config firewall address
  edit "aws-address-1"
    set type dynamic
    set sdn "aws1"
    set filter "Tag.Name=aws*"
    set sdn-addr-type public
  next
end
```

2. Create the dynamic firewall address and verify where the IP addresses resolve to:

```
config firewall address
  edit "aws-address-1"
    set type dynamic
    set sdn "aws1"
```

```
set filter "Tag.Name=aws*"
set sdn-addr-type public
config list
  edit "18.234.167.123"
  next
  edit "3.81.41.167"
  next
  edit "52.87.157.127"
  next
end
next
end
```

3. In AWS, verify that the IP addresses match.

Kubernetes (K8s) SDN connectors

The following topics provide information about configuring Kubernetes SDN connectors:

- [Private Cloud K8s SDN connector on page 182](#)
- [AWS Kubernetes \(EKS\) SDN connector on page 186](#)
- [Azure Kubernetes \(AKS\) SDN connector on page 191](#)
- [GCP Kubernetes \(GKE\) SDN connector on page 188](#)
- [Oracle Kubernetes \(OKE\) SDN connector on page 194](#)

Private Cloud K8s SDN connector

FortiOS automatically updates dynamic and cluster IP addresses for Kubernetes (K8s) by using a K8s SDN connector, enabling FortiOS to manage K8s pods as global address objects, as with other connectors. This includes mapping the following attributes from K8s instances to dynamic address groups in FortiOS:

Filter	Description
Namespace	Filter service IP addresses in a given namespace.
ServiceName	Filter service IP addresses by the given service name.
NodeName	Filter node IP addresses by the given node name.
PodName	Filter IP addresses by the pod name.
Label.XXX	Filter service or node IP addresses with the given label XXX. For example: <code>K8S_Label.app=nginx</code> .

FortiOS 6.2.3 and later collects cluster IP addresses in addition to external IP addresses for exposed K8s services.



There is no maximum limit for the number of IP addresses populated with the filters.

To obtain the IP address, port, and secret token in K8s:

1. When configuring the K8s SDN connector in FortiOS, you must provide the IP address and port that the K8s deployment is running on. Run `kubectl cluster-info` to obtain the IP address and port. Note down the IP address and port. The following shows the IP address and port for a local cluster:

```
[root@k8smaster ~]# kubectl cluster-info
Kubernetes master is running at https://172.17.215.10:6443
KubeDNS is running at https://172.17.215.10:6443/api/v1/namespaces/kube-system/services/kube-dns:dns/proxy
```

The following shows the IP address and port for customer-managed K8s on Google Cloud Platform:

```
root@kali:~# ssh -i /root/.ssh/google_compute_engine dev-project-001-166400@cloudshell:~ (dev-project-001-166400)$ kubectl cluster-info
Kubernetes master is running at https://35.227.148.44
GLBCDefaultBackend is running at https://35.227.148.44/api/v1/namespaces/kube-system/services/default-http-backend:http/proxy
```

2. Generate the authentication token:

- a. Create a service account to store the authentication token:
 - i. Run the `kubectl create serviceaccount <Service_account_name>` command. For example, if the service account name is `fortigateconnector`, the command is `kubectl create serviceaccount fortigateconnector`.
 - ii. Run the `kubectl get serviceaccounts` command to verify that you created the service account. The account should show up in the service account list.
- b. Create a cluster role. K8s 1.6 and later versions allow you to configure role-based access control (RBAC). RBAC is an authorization mechanism to manage resource permissions on K8s. You must create a cluster role to grant the FortiGate permission to perform operations and retrieve objects:
 - i. Create the yaml file by running the `vi <filename>.yaml` command. For example, if the yaml file name is `fgtclusterrole`, the command is `vi fgtclusterrole.yaml`. Paste the following:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  # "namespace" omitted since ClusterRoles are not namespaced
  name: fgt-connector

rules:
- apiGroups: [""]

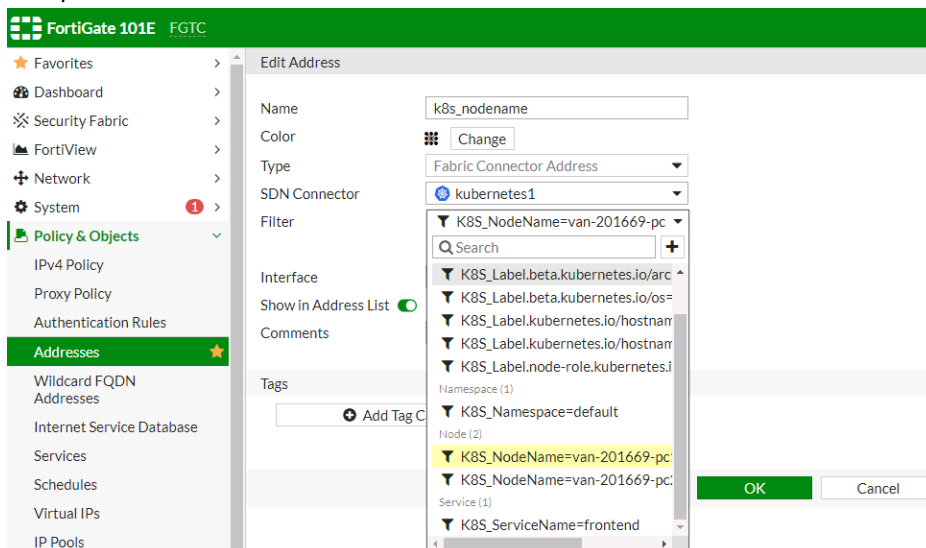
  resources: ["pods", "namespaces", "nodes" , "services"]
  verbs: ["get", "watch", "list"]
```

The resources list specifies the objects that FortiOS can retrieve. The verbs list specifies the operations that FortiOS can perform.

- ii. Run the `Kubectl apply -f <filename>.yaml` command to apply the yaml file to create the cluster role. In this example, the command is `Kubectl apply -f fgtclusterrole.yaml`.
 - iii. Run the `kubectl create clusterrolebinding fgt-connector --clusterrole=<cluster_role_name> --serviceaccount=default:<service_account_name>` to attach the cluster role to the service account. In this example, the command is `kubectl create clusterrolebinding fgt-connector --clusterrole=fgt-connector --serviceaccount=default:fortigateconnector`.
- c. Run the `kubectl get secrets -o jsonpath='{.items[?(@.metadata.annotations['kubernetes.io/service-account.name']=='fortigateconnector')].data.token}' | base64 --decode` command to obtain the secret token. As the token is Base64 encoded, the command includes `base64 --decode` to extract the decoded keystring. Note down the token.

To configure K8s SDN connector using the GUI:

1. Configure the K8s SDN connector:
 - a. Go to *Security Fabric > External Connectors > Create New Connector*.
 - b. Select *Kubernetes*.
 - c. In the *IP* field, enter the IP address that you obtained in [To obtain the IP address, port, and secret token in K8s: on page 183](#).
 - d. In the *Port* field, select *Specify*, then enter the port that you obtained in [To obtain the IP address, port, and secret token in K8s: on page 183](#).
 - e. In the *Secret token* field, enter the token that you obtained in [To obtain the IP address, port, and secret token in K8s: on page 183](#).
 - f. Configure the other fields as desired.
2. Create a dynamic firewall address for the configured K8S SDN connector:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Click *Create New*, then select *Address*.
 - c. Configure the address as shown, selecting the desired filter in the *Filter* dropdown list. In this example, the K8s SDN connector will automatically populate and update IP addresses only for node instances that match the specified node name:



3. Ensure that the K8s SDN connector resolves dynamic firewall IP addresses:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Hover over the address created in step 2 to see a list of IP addresses for node instances that match the node

name configured in step 2:

Name	Type
aws-security	Fabric Connector Address (AWS)
aws-zone	Fabric Connector Address (AWS)
az-k8s-cluster	Fabric Connector Address (AZURE)
az-k8s-label	Fabric Connector Address (AZURE)
az-k8s-pod	Fabric Connector Address (AZURE)
az-k8s-region	Fabric Connector Address (AZURE)
dmz	Interface Subnet
gmail.com	FQDN
google-play	DN
k8s_label	Fabric Connector Address (KUBERNETES)
k8s_nodename	Fabric Connector Address (KUBERNETES)

Tooltip for k8s_nodename: k8s_nodename resolves to:
• 172.16.65.227

To configure K8s SDN connector using CLI commands:

1. Configure the K8s SDN connector:

```
config system sdn-connector
  edit "kubernetes1"
    set type kubernetes
    set server "<IP address obtained in To obtain the IP address, port, and secret token in K8s: on page 183>"
    set server-port <Port obtained in To obtain the IP address, port, and secret token in K8s: on page 183>
    set secret-token <Secret token obtained in To obtain the IP address, port, and secret token in K8s: on page 183>
    set update-interval 30
  next
end
```

2. Create a dynamic firewall address for the configured K8s SDN connector with the supported K8s filter. In this example, the K8s SDN connector will automatically populate and update IP addresses only for node instances that match the specified node name:

```
config firewall address
  edit "k8s_nodename"
    set type dynamic
    set sdn "kubernetes1"
    set filter "K8S_NodeName=van-201669-pc1"
  next
end
```

3. Confirm that the K8s SDN connector resolves dynamic firewall IP addresses using the configured filter:

```
config firewall address
  edit "k8s_nodename"
    set type dynamic
    set sdn "kubernetes1"
    set filter "K8S_NodeName=van-201669-pc1"
    config list
      edit "172.16.65.227"
    next
  end
next
end
```

To troubleshoot the connection:

1. In FortiOS, run the following commands:

```
diagnose deb application kubed -1
diagnose debug enable
```
2. Reset the connection on the web UI to generate logs and troubleshoot the issue. The following shows the output in the case of a failure:

```
fortigate # diagnose deb application kubed -1
Debug messages will be on for 30 minutes.

fortigate # diagnose debug enable

fortigate # k8s: update sdn connector kubernetes1 status to enabled
k8s: update sdn connector kubernetes2 status to disabled
kubed sdn connector kubernetes1 prepare to update
getting token
kubed sdn connector kubernetes1 start updating
kube url: https://172.17.215.10:6443/api/v1/services
kube host: 172.17.215.10:6443:172.17.215.10
{"kind": "Status", "apiVersion": "v1", "metadata": {}, "status": "Failure", "message": "services is forbidden: User \"system:serviceaccount:default:fortigateconnector\" cannot list resource \"services\" in API group \"\" at the cluster scope", "reason": "Forbidden", "details": {"kind": "services"}, "code": 403}

kubed failed to list kubernetes services.
kubed failed to get IPs from kubedrnets services.
kubed failed to get ip addr list
kubed reap child pid: 1226
```

The following shows the output in the case of a success:

```
kube-system
k8s pod ip: 10.180.1.2, podname: metrics-server-v0.3.6-64655c969-djt8s, namespace: kube-system
k8s pod ip: 10.138.0.6, podname: netd-4qvvn, namespace: kube-system
k8s pod ip: 10.138.0.5, podname: netd-756ch, namespace: kube-system
k8s pod ip: 10.138.0.4, podname: netd-hr75d, namespace: kube-system
k8s pod ip: 10.138.0.6, podname: prometheus-to-sd-59trp, namespace: kube-system
k8s pod ip: 10.138.0.4, podname: prometheus-to-sd-q6qv5, namespace: kube-system
k8s pod ip: 10.138.0.5, podname: prometheus-to-sd-rq2zm, namespace: kube-system
k8s pod ip: 10.180.1.3, podname: stackdriver-metadata-agent-cluster-level-6c4f64f8cc-zgnp5, namespace: kube-system
k8s pod ip: 10.180.0.3, podname: nginx-deployment-c68885cbb-sf6f5, namespace: nginx
k8s pod ip: 10.180.1.4, podname: nginx-deployment-c68885cbb-w5w2b, namespace: nginx
kubed get IP address list from Kubernetes:
kubed sdn connector kubernetes2 start updating IP addresses
kubed checking firewall address object gcp-address, v0 0
address num change 0/3, new ip list:
10.180.0.3
10.180.1.4
10.184.0.1
kubed sdn connector kubernetes2 finish updating IP addresses
kubed reap child pid: 1252
```

AWS Kubernetes (EKS) SDN connector

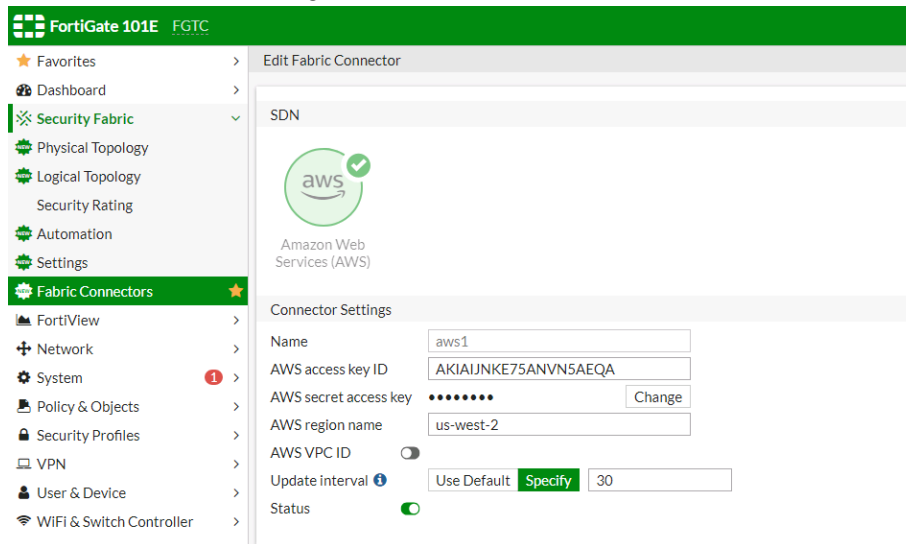
AWS SDN connectors support dynamic address groups based on AWS Kubernetes (EKS) filters.

To filter out the Kubernetes IP addresses, the following address filters have been introduced:

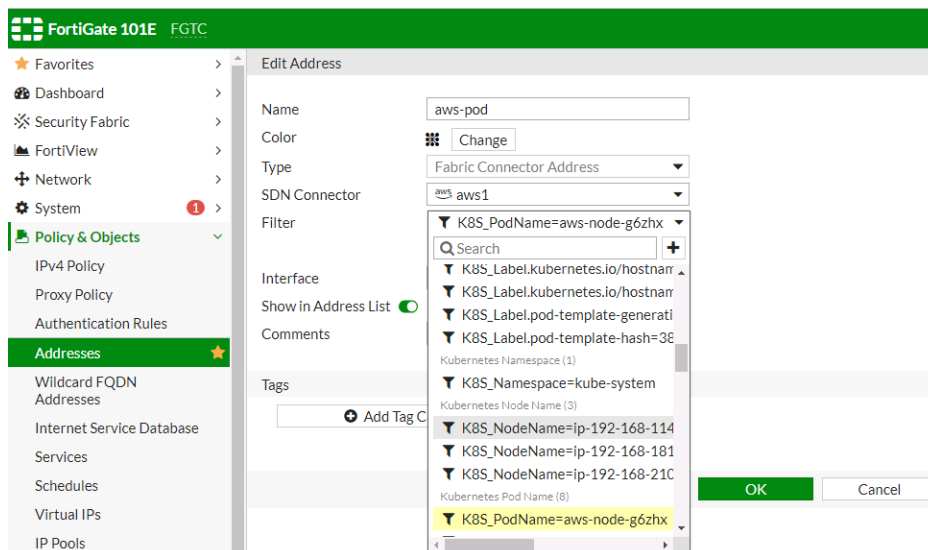
k8s_cluster	Name of Kubernetes cluster.
k8s_namespace	Namespace of a Kubernetes service or pod.
k8s_svcname	Name of a Kubernetes service.
k8s_nodename	Name of a Kubernetes node.
k8s_zone	Zone of a Kubernetes node.
k8s_region	Region of a Kubernetes node.
k8s_podname	Name of a Kubernetes pod.
k8s_label.xxx	Name of label of a Kubernetes resource (cluster/service/node/Pod).

To enable an AWS SDN connector to fetch IP addresses from AWS Kubernetes:

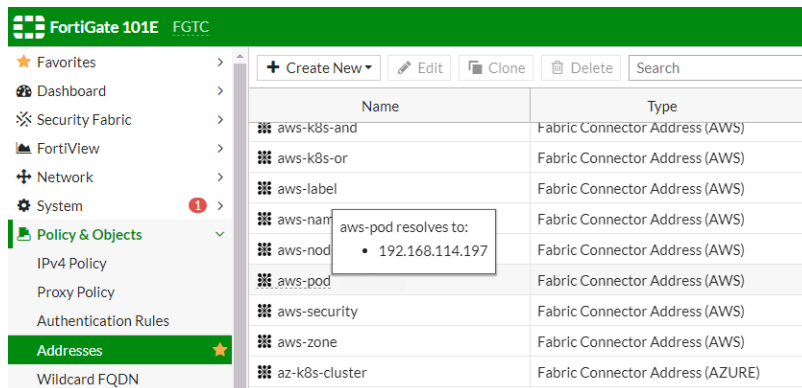
1. In *Fabric Connectors*, configure an SDN connector for AWS Kubernetes.



2. Go to *Policies & Objects > Addresses* and create a dynamic firewall address for the configured SDN connector using the supported Kubernetes filter.
3. To filter out the Kubernetes IP addresses, select the address filter or filters.



4. Configure the rest of the settings, then click **OK**.
The dynamic firewall address IP is resolved by the SDN connector.



To configure an AWS Kubernetes SDN connector through the CLI:

1. Configure an SDN connector for Kubernetes:

```
config system sdn-connector
  edit "aws1"
    set type aws
    set access-key "AKIAIJNKE75ANVN5AEQA"
    set secret-key xxxxx
    set region "us-west-2"
    set update-interval 30
  next
end
```

2. Create a dynamic firewall address for the SDN connector with a supported Kubernetes filter:

```
config firewall address
  edit "aws-pod"
    set type dynamic
    set sdn "aws1"
    set filter "K8S_PodName=aws-node-g6zhx"
  next
end
```

The dynamic firewall address IP is resolved by the SDN connector:

```
config firewall address
  edit "aws-pod"
    set uuid a7a37298-19e6-51e9-851a-2c551ffc174d
    set type dynamic
    set sdn "aws1"
    set filter "K8S_PodName=aws-node-g6zhx"
    config list
      edit "192.168.114.197"
    next
  end
next
end
```

GCP Kubernetes (GKE) SDN connector

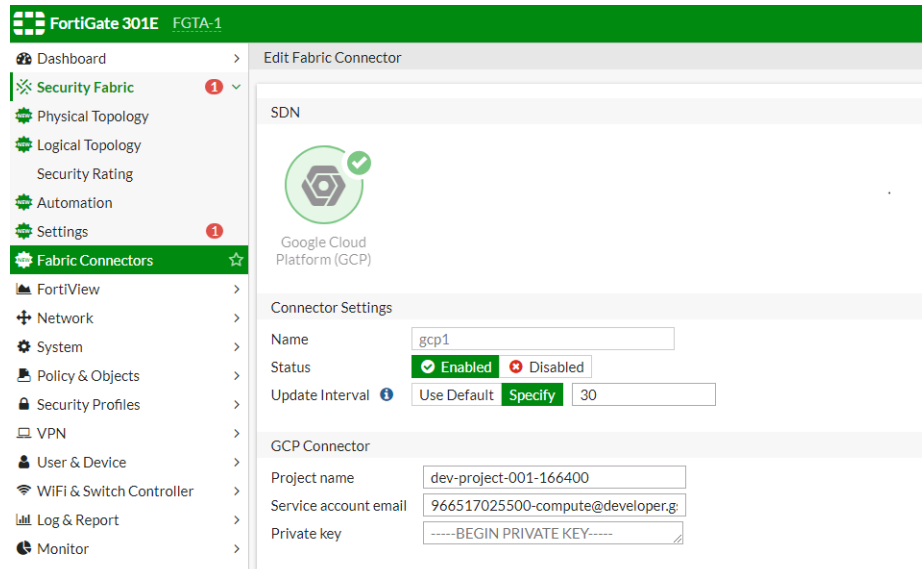
Google Cloud Platform (GCP) SDN connectors support dynamic address groups based on GCP Kubernetes Engine (GKE) filters.

To filter out the Kubernetes IP addresses, the following address filters have been introduced:

k8s_cluster	Name of Kubernetes cluster.
k8s_nodepool	Name of node pool for a Kubernetes cluster.
k8s_namespace	Namespace of a Kubernetes service or pod.
k8s_servicename	Name of a Kubernetes service.
k8s_nodename	Name of a Kubernetes node.
k8s_zone	Zone of a Kubernetes node.
k8s_region	Region of a Kubernetes node.
k8s_podname	Name of a Kubernetes pod.
k8s_label.xxx	Name of label of a Kubernetes resource (cluster/service/node/Pod).

To enable a GCP SDN connector to fetch IP addresses from GKE:

1. In *Fabric Connectors*, configure an SDN connector for GCP.



2. Go to *Policies & Objects > Addresses* and create a dynamic firewall address for the configured SDN connector using the supported Kubernetes filter.
3. To filter out the Kubernetes IP addresses, select the address filter or filters. In this example, the GCP SDN connector will automatically populate and update IP addresses only for instances that belong to the zhm-kc3 cluster:

- Configure the rest of the settings, then click **OK**.
The dynamic firewall address IP is resolved by the SDN connector.

Name	Type
Address 13	
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet
SSLVPN_TUNNEL_ADDR1	IP Range
all	Subnet
gcp-k8s-cluster	Fabric Connector Address (GCP)
gcp-k8s-label	gcp-k8s-cluster resolves to:
gcp-k8s-pod	10.0.2.4
gcp-k8s-pool	10.0.2.7
gmail.com	10.28.0.13
login.microsoft	10.28.0.14
login.microsoft	10.28.0.17
login.microsoft	10.28.0.18
login.microsoft	10.28.0.19
login.microsoft	10.28.0.20
login.microsoft	10.28.0.21
login.microsoft	10.28.0.22
login.microsoft	10.28.1.11
login.microsoft	10.28.1.12
login.microsoft	10.28.1.13
login.microsoft	10.28.1.14
login.microsoft	10.28.1.15
login.microsoft	35.235.101.176
login.microsoft	35.236.43.119
login.microsoft	35.236.60.13
login.microsoft	50.13.123.45
Address Group	
Wildcard FQDN	

To configure a GCP Kubernetes SDN connector through the CLI:

- Configure an SDN connector for Kubernetes:


```
config system sdn-connector
    edit "gcp1"
      set type gcp
      set gcp-project "dev-project-001-166400"
      set service-account "966517025500-compute@developer.gserviceaccount.com"
      set update-interval 30
    next
end
```
- Create a dynamic firewall address for the SDN connector with a supported Kubernetes filter:


```
config firewall address
    edit "gcp-k8s-cluster"
```

```

        set type dynamic
        set sdn "gcp1"
        set filter "K8S_Cluster=zhm-kc3"
    next
end

```

The dynamic firewall address IP is resolved by the SDN connector:

```

config firewall address
    edit "gcp-k8s-cluster"
        set uuid e4a1aa3c-25be-51e9-e9af-78ab2eebe6ee
        set type dynamic
        set sdn "gcp1"
        set filter "K8S_Cluster=zhm-kc3"
    config list
        edit "10.0.2.4"
        next
        edit "10.0.2.7"
        next
        edit "10.28.0.13"
        next
    end
next
end

```

Azure Kubernetes (AKS) SDN connector

Azure SDN connectors support dynamic address groups based on Azure Kubernetes (AKS) filters.

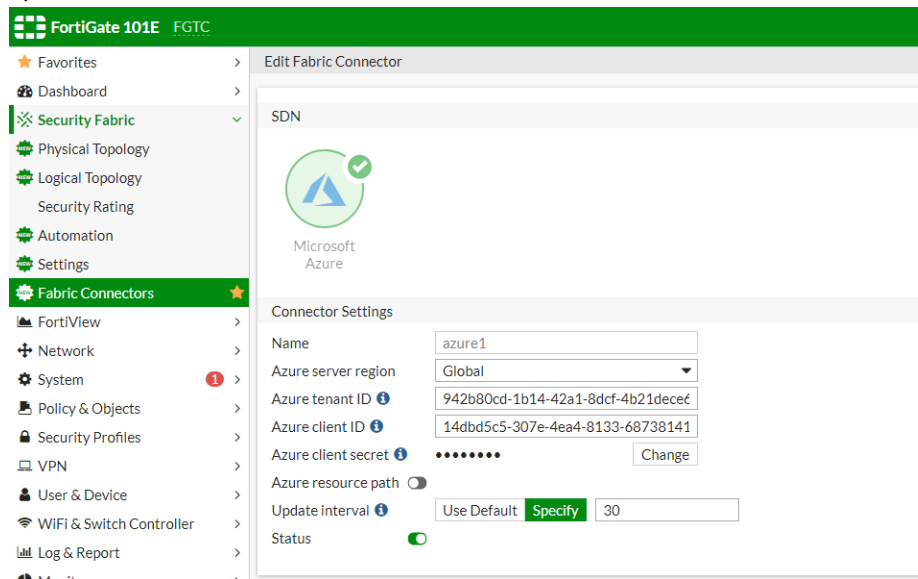
To filter out the Kubernetes IP addresses, the following address filters have been introduced:

k8s_cluster	Kubernetes cluster name.
k8s_namespace	Namespace of a Kubernetes service or pod.
k8s_svcname	Kubernetes service name.
k8s_nodename	Kubernetes node name.
k8s_region	Kubernetes node region.
k8s_podname	Kubernetes pod name.
k8s_label.xxx	Name of label of a Kubernetes resource (cluster/service/node/Pod).

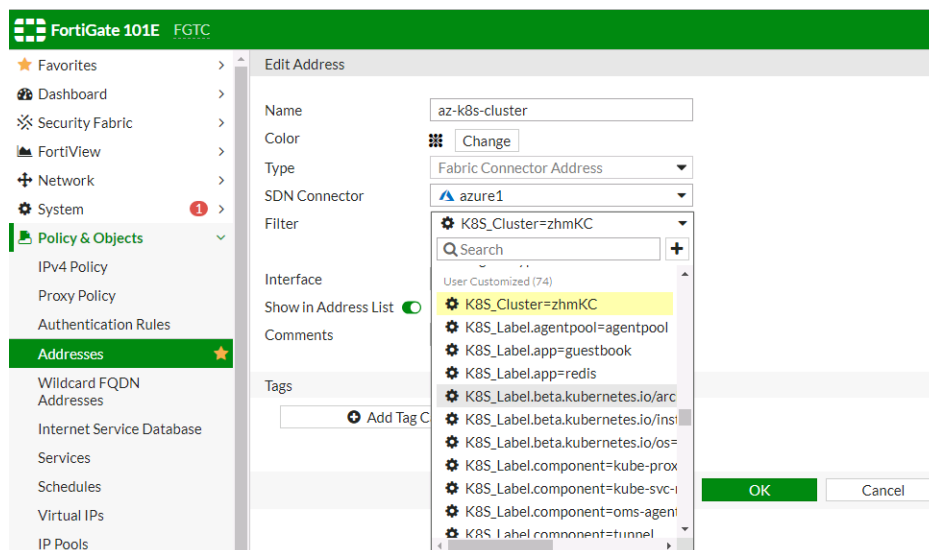
To enable an Azure SDN connector to fetch IP addresses from Azure Kubernetes:

1. Configure the Azure SDN connector:
 - a. Go to *Security Fabric > Fabric Connectors*.
 - b. Click *Create New*, and select *Azure*.
 - c. Configure as shown substituting the region, tenant and client IDs, and client secret for your deployment. The

update interval is in seconds.

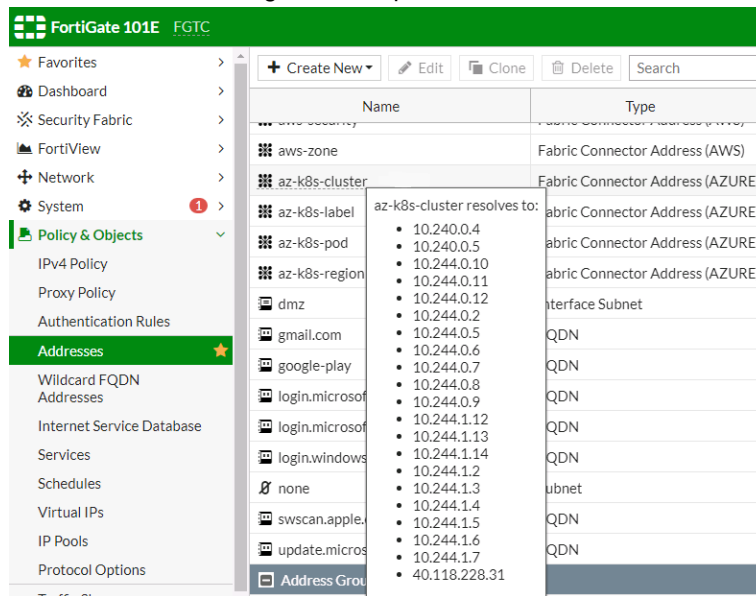


2. Create a dynamic firewall address for the configured K8S SDN connector:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Click *Create New*, then select *Address*.
 - c. Configure the address as shown, selecting the desired filter in the *Filter* dropdown list. In this example, the Azure SDN connector will automatically populate and update IP addresses only for instances that belong to the zhmKC cluster:



3. Ensure that the K8S SDN connector resolves dynamic firewall IP addresses:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Hover over the address created in step 2 to see a list of IP addresses for instances that belong to the

zhmKC cluster as configured in step 2:



To configure an Azure Kubernetes SDN connector through the CLI:

1. Configure an SDN connector for Kubernetes:

```
config system sdn-connector
  edit "azure1"
    set type azure
    set tenant-id "942b80cd-1b14-42a1-8dcf-4b21dece61ba"
    set client-id "14dbd5c5-307e-4ea4-8133-68738141feb1"
    set client-secret xxxxxx
    set update-interval 30
  next
end
```

2. Create a dynamic firewall address for the SDN connector with a supported Kubernetes filter. In this example, the Azure SDN connector will automatically populate and update IP addresses only for instances that belong to the zhmKC cluster:

```
config firewall address
  edit "az-k8s-cluster"
    set type dynamic
    set sdn "azure1"
    set filter "K8S_Cluster=zhmKC"
  next
end
```

3. Confirm that the Azure SDN connector resolves dynamic firewall IP addresses using the configured filter: :

```
config firewall address
  edit "az-k8s-cluster"
    set uuid c3859270-1919-51e9-4a99-47d8caf97a01
    set type dynamic
    set sdn "azure1"
    set filter "K8S_Cluster=zhmKC"
  config list
    edit "10.240.0.4"
    next
    edit "10.240.0.5"
```

```
        next
        edit "10.244.0.10"
        next
    end
next
end
```

Oracle Kubernetes (OKE) SDN connector

OCI SDN connectors support dynamic address groups based on Oracle Kubernetes (OKE) filters.

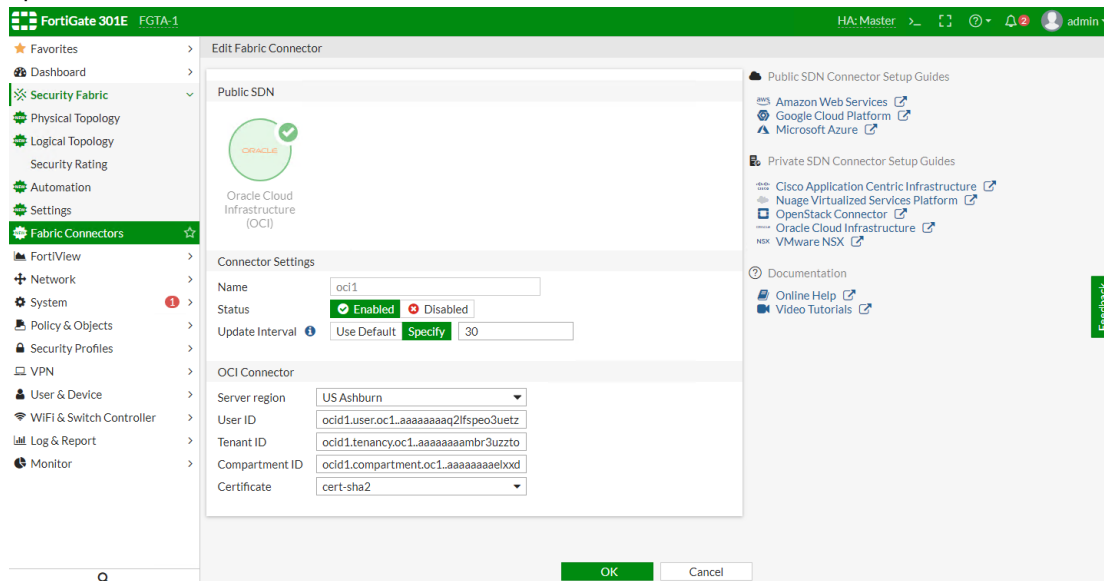
To filter out the Kubernetes IP addresses, the following address filters have been introduced:

k8s_compartment	Name of compartment that the Kubernetes cluster created in.
k8s_cluster	Name of Kubernetes cluster.
k8s_namespace	Namespace of a Kubernetes service or pod.
k8s_servicename	Name of a Kubernetes service.
k8s_nodename	Name of a Kubernetes node.
k8s_region	Region of a Kubernetes node.
k8s_zone	Zone of a Kubernetes node.
k8s_podname	name of a Kubernetes pod.
k8s_label.xxx	Name of label of a Kubernetes resource (cluster/service/node/Pod)

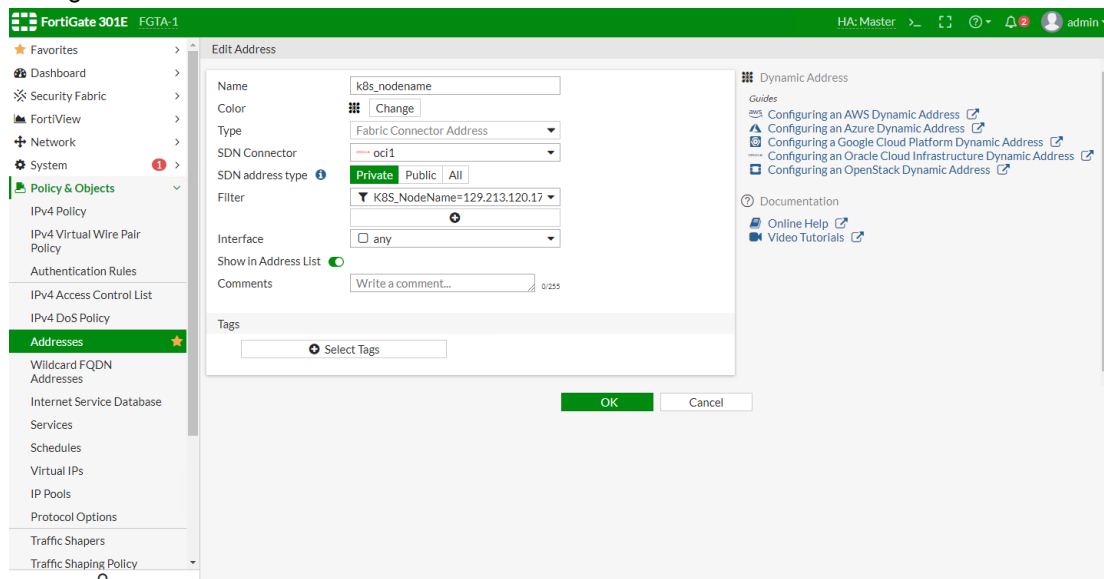
To enable an OCI SDN connector to fetch IP addresses from Oracle Kubernetes:

1. Configure the OCI SDN connector:
 - a. Go to *Security Fabric > Fabric Connectors*.
 - b. Click *Create New*, and select *Oracle Cloud Infrastructure (OCI)*.
 - c. Configure as shown substituting the region, tenant and client IDs, and client secret for your deployment. The

update interval is in seconds.

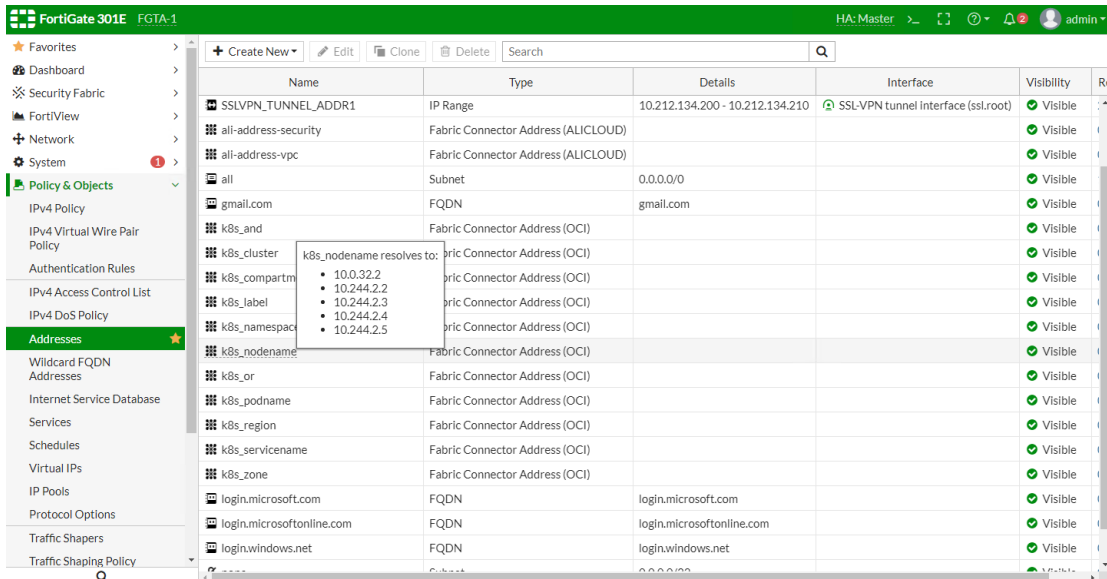


2. Create dynamic firewall addresses for the configured SDN connector with supported Kubernetes filter:
 - a. Go to *Policy & Objects > Addresses*.
 - b. Click *Create New*, then select *Address*.
 - c. Configure the addresses.



3. Confirm that the SDN connector resolves dynamic firewall IP addresses:

- Go to *Policy & Objects > Addresses*.
- Hover over the address created in step 2 to see a list of IP addresses for instances:



To configure an SDN connector through the CLI:

1. Configure the OCI SDN connector:

```
config system sdn-connector
edit "oci1"
set type oci
set tenant-id
"ocid1.tenancy.oc1..aaaaaaaambr3uzztoyhweohbzqqdo775h7d3t54zpmz4b2cf35vs5
5cxxx"
set user-id
"ocid1.user.oc1..aaaaaaaq21fspeo3uetzbzpiv2pqvzvevozccnys347stwssvizqlatfx
xx"
set compartment-id
"ocid1.compartment.oc1..aaaaaaaalxxdjazqo7nzcpgypiyqcgkmytjry6nfg5345vw7e
avpwnmxxx"
set oci-region ashburn
set oci-cert "cert-sha2"
set update-interval 30
next
end
```

2. Create dynamic firewall addresses for the configured SDN connector with supported Kubernetes filter:

```
config firewall address
edit "k8s_nodeName"
set type dynamic
set sdn "oci1"
set filter "K8S_NodeName=129.213.120.172"
next
end
```

3. Confirm that the SDN connector resolves dynamic firewall IP addresses:

```
config firewall address
edit "k8s_nodeName"
set uuid 052f1420-3ab8-51e9-0cf8-6db6bc3395c0
```

```
set type dynamic
set sdn "oci1"
set filter "K8S_NodeName=129.213.120.172"
config list
  edit "10.0.32.2"
  next
  edit "10.244.2.2"
  next
  edit "10.244.2.3"
  next
  edit "10.244.2.4"
  next
  edit "10.244.2.5"
  next
end
next
end
```

SSO/Identity connectors

SSO fabric connectors integrate SSO authentication into the network. This allows users to enter their credentials only once, and have those credentials reused when accessing other network resources through the FortiGate.

The following fabric connectors are available:

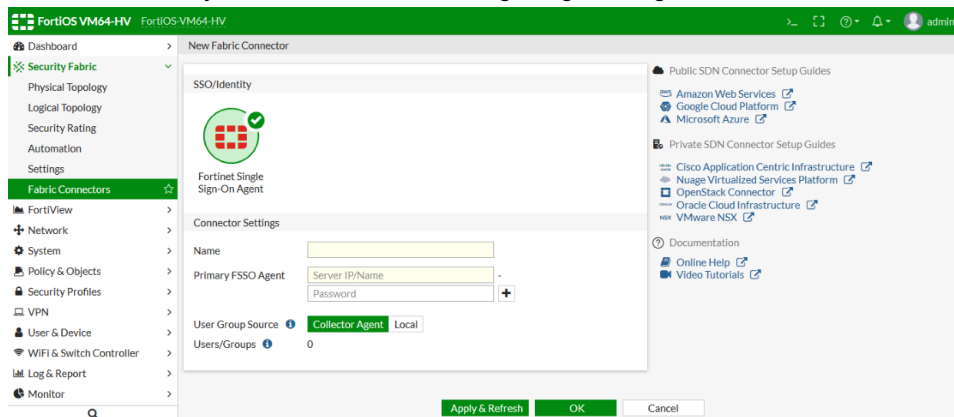
- [Fortinet single sign-on agent on page 197](#)
- [Poll Active Directory server on page 198](#)
- [FortiClient EMS connector on page 199](#)
- [FortiNAC endpoint connector on page 201](#)
- [Symantec endpoint connector on page 207](#)
- [RADIUS single sign-on \(RSSO\) agent on page 214](#)

Fortinet single sign-on agent

To create an FSSO agent connector in the GUI:

1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New*.

3. In the *SSO/Identity* section, click *Fortinet Single Sign-On Agent*.



4. Fill in the *Name*, and *Primary FSSO Agent* server IP address or name and *Password*.

5. Optionally, add more FSSO agents by clicking the plus icon.

6. Select the *User Group Source*:

- **Collector Agent:** User groups will be pushed to the FortiGate from the collector agent. Click *Apply & Refresh* to fetch group filters from the collector agent.
- **Local:** User groups will be specified in the FortiGate unit's configuration. Select the LDAP server from the drop-down list, then select the *Users*, *Groups*, and *Organizational Units*. Enable or disable *Recursive* as required.

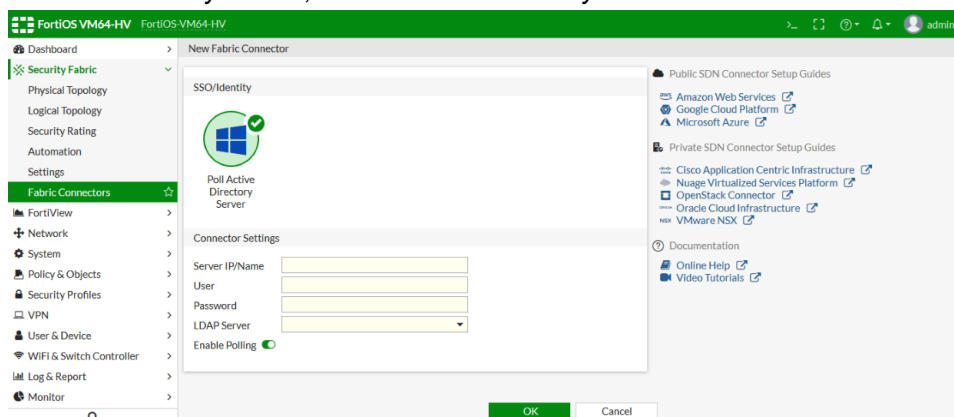
7. Click *OK*.

Poll Active Directory server

The FortiGate unit can authenticate users and allow them network access based on groups membership in Windows Active Directory (AD).

To create an AD server connector in the GUI:

1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New*.
3. In the *SSO/Identity* section, click *Poll Active Directory Server*.



4. Fill in the *Server IP/Name*, *User*, and *Password* for the AD server.

5. Select the LDAP server from the list.

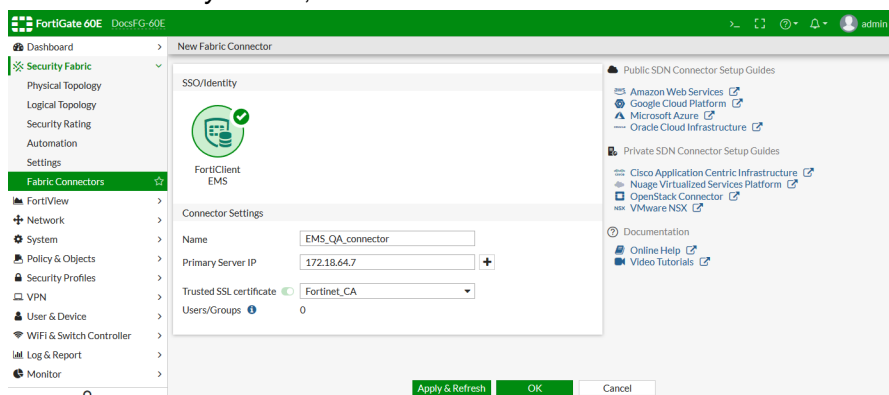
6. If necessary, disable *Enable Polling*. This can be used to temporarily stop the FortiGate from polling security event logs on the Windows logon server, for troubleshooting purposes.
7. Click **OK**.

FortiClient EMS connector

This example describes how to create a FortiClient EMS connector and a user group for the connector.

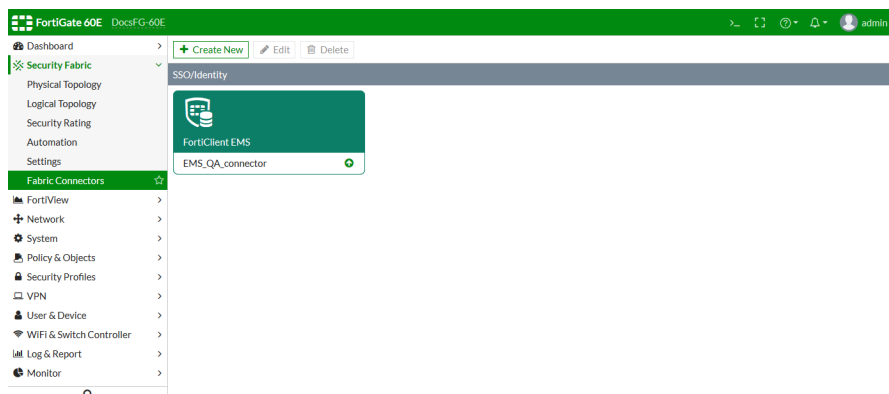
To create an FortiClient EMS connector in the GUI:

1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New*.
3. In the *SSO/Identity* section, click *FortiClient EMS*.



4. Fill in the *Name*, and *Primary Server IP*, and select a *Trusted SSL certificate*.
5. Click **OK**.

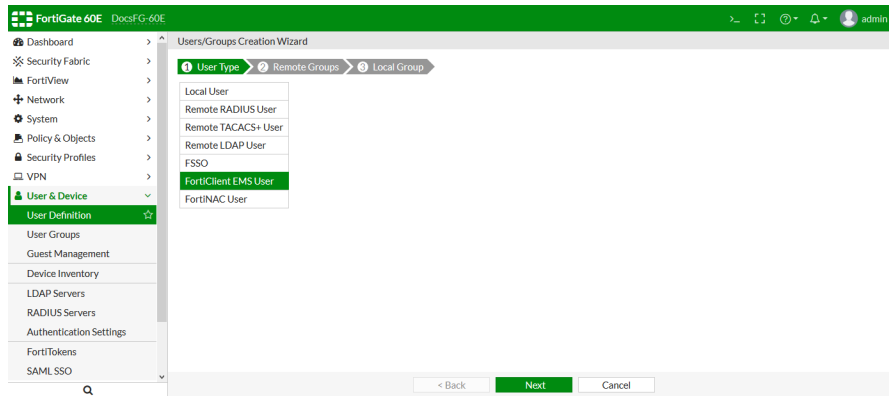
The connector is shown on the *Fabric Connectors* page.



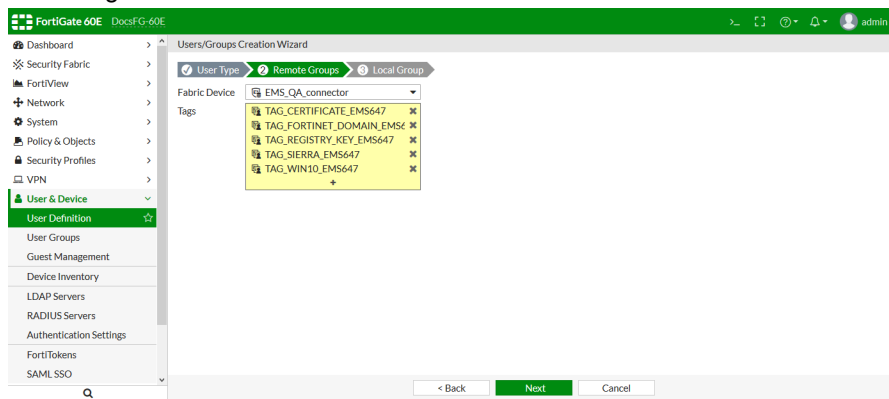
To create a user group for the EMS fabric connector using the GUI:

1. Go to *User & Device > User Definition*.
2. Click *Create New*.

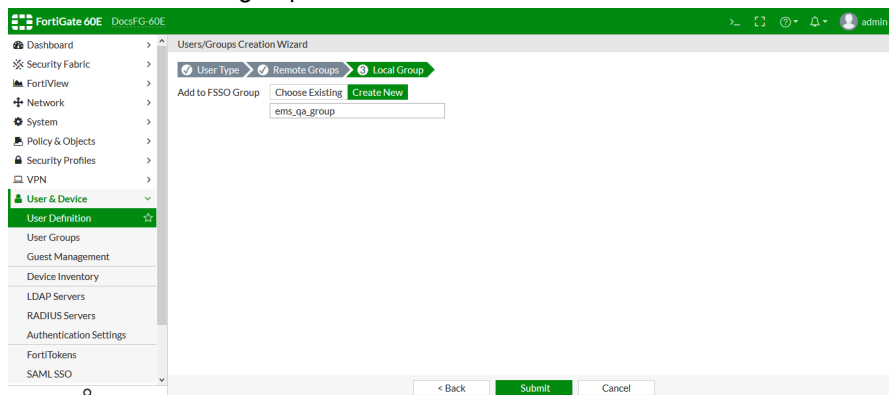
3. Select *FortiClient EMS User*, then click *Next*.



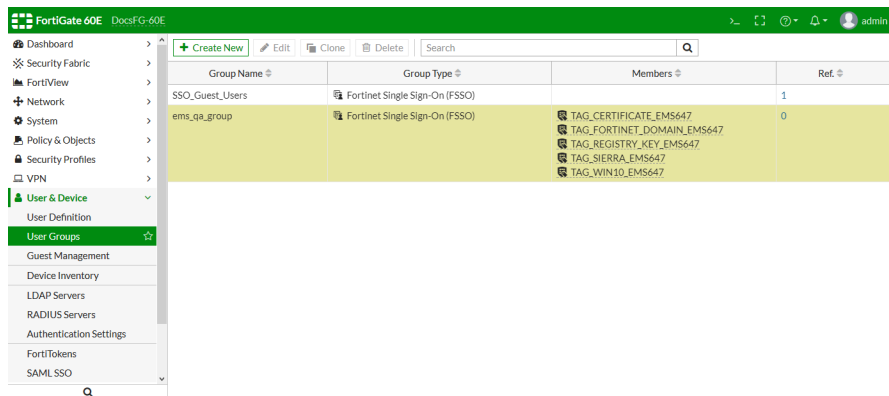
4. In the *Fabric Device* list select the EMS fabric connector that you created.
5. Select tags and then click *Next*.



6. In the *Add to FSSO Group* field, click *Create New*.
7. Enter a name for the group.



8. Click *Submit*.
- The configured group is shown at *User & Device > User Groups*.



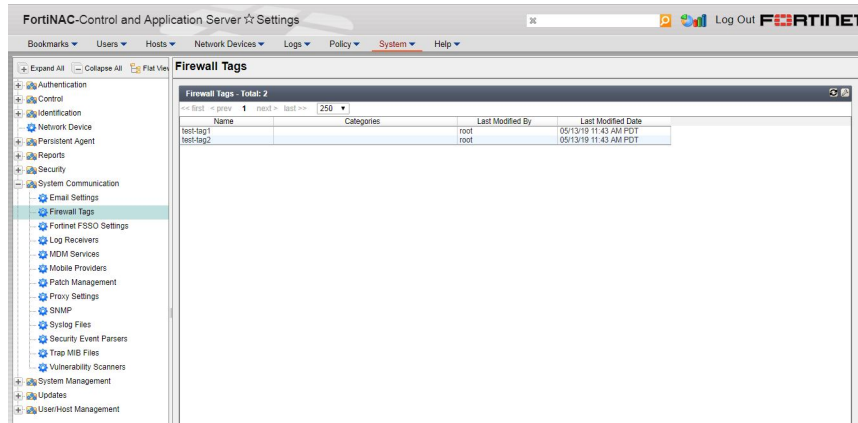
FortiNAC endpoint connector

Dynamic address definitions originating from FortiNAC can be imported to FortiGate as FSSO objects and used in firewall policies. Changes on the FortiNAC are dynamically reflected on the FortiGate.

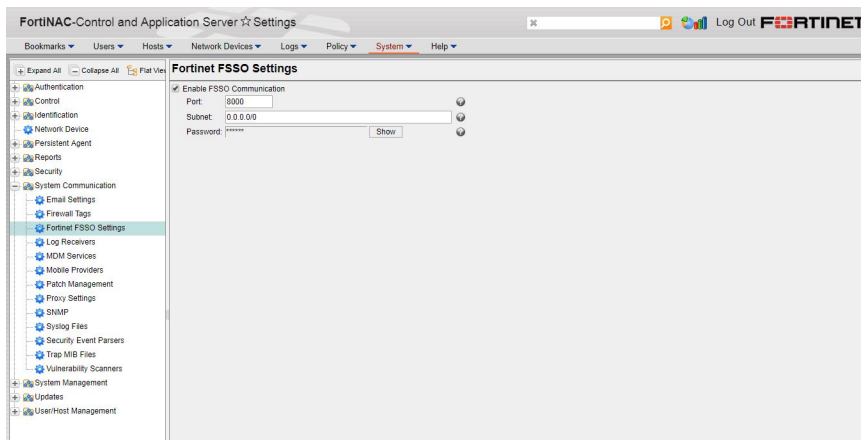
This example assumes that the FortiGate and FortiNAC are in the same network segment. If layer 3 routers or firewalls are in between them, ensure that traffic on port 8000 is not blocked.

Configuring the FortiNAC

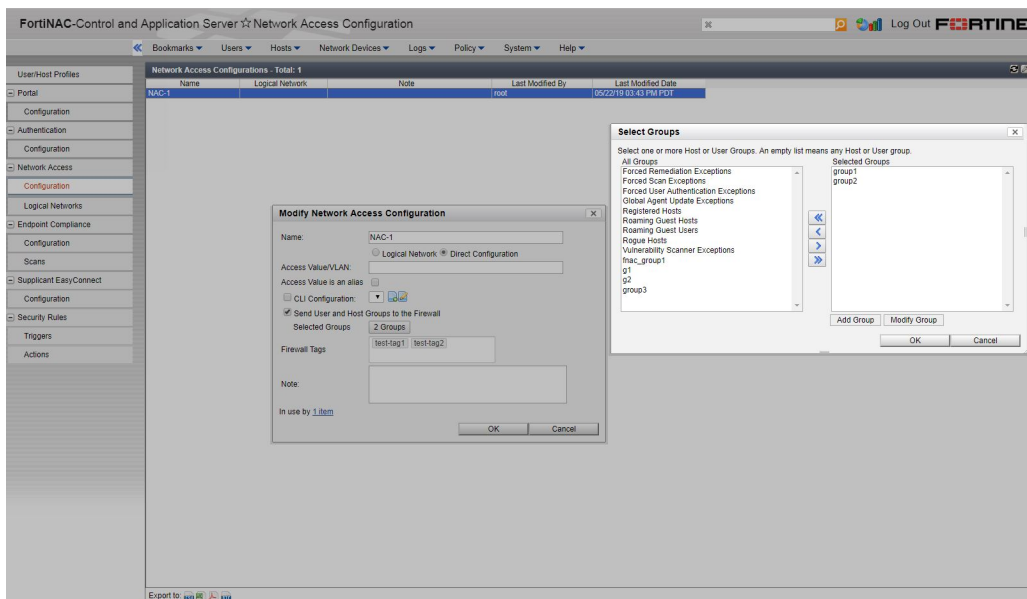
On FortiNAC, local groups and users can be created, and they can be imported from remote servers, such as AD LDAP and RADIUS servers. Local firewall tags, used in FortiNAC policies, are also supported.



Before creating the FortiNAC connector on the FortiGate, FSSO must be enabled:



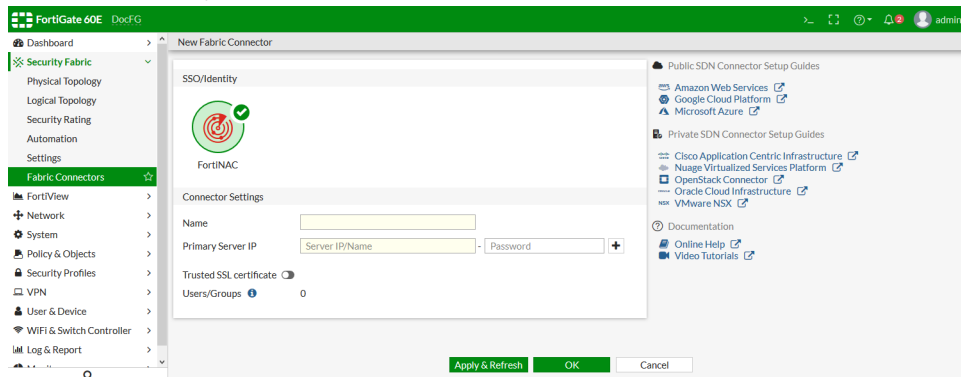
Groups and firewall tags that will be monitored and accessed by the FortiGate must be added to a network access policy on the FortiNAC:



Configuring the FortiGate

To configure the FortiNAC connector in the GUI:

1. Go to *Security Fabric > Fabric Connectors* and click *Create New*.
2. In the *SSO/Identity* section, click *FortiNAC*.

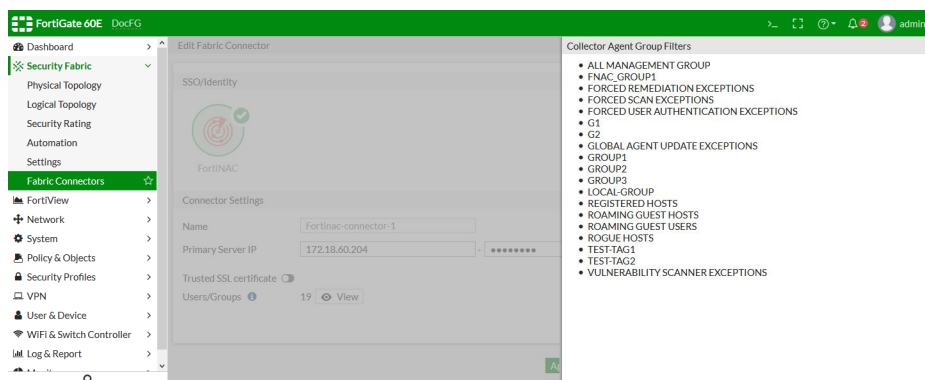


3. Enter a name for the connector in the *Name* field, such as *Fortinac-connector-1*.
4. Enter the FortiNAC device's IP address and password in the *Primary Server IP* fields.
5. Click *Apply & Refresh*.

All host groups, firewall tags, and some default system groups will be pushed to the FortiGate from the FortiNAC.

6. Click *View*.

The *Collector Agent Group Filters* pane opens, showing the information pushed from FortiNAC. These objects can be used to create FSSO user groups.



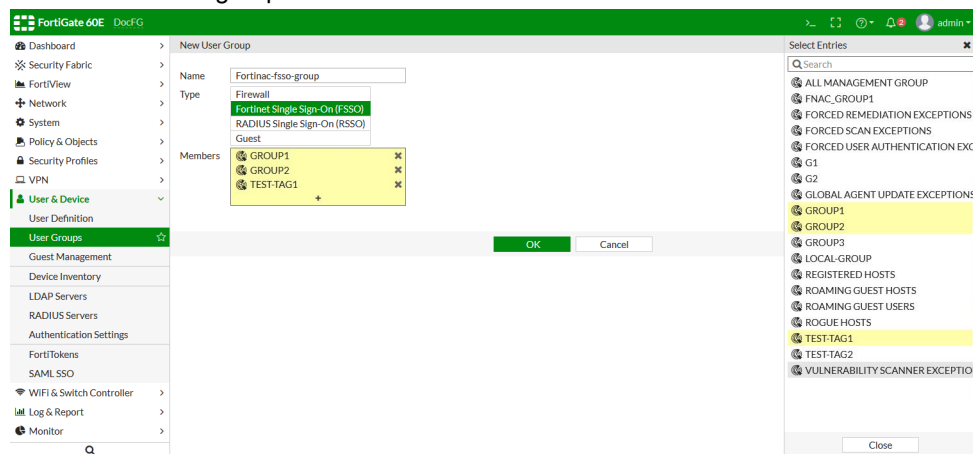
7. Click *OK*.

To configure the FortiNAC connector in the CLI:

```
config user fssso
  edit "Fortinac-connector-1"
    set server "172.18.60.204"
    set password XXXXXXXXXXXXXXXXXX
    set type fortinac
  next
end
```

To create an FSSO user group using imported FortiNAC groups and tags as members in the GUI:

1. Go to *User & Device > User Groups*.
2. Click *Create New*.
3. In the *Name* field, enter a name for the group, such as *Fortinac-fsso-group*.
4. For *Type*, select *Fortinet Single Sign-On (FSSO)*.
5. In the *Members* field, click +. The *Select Entries* pane appears. The groups and tags pulled from the FortiNAC are shown.
6. Select the desired groups.



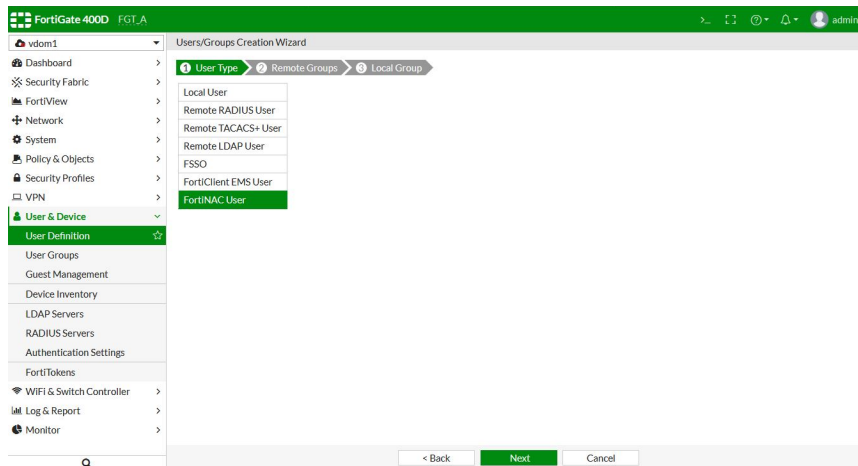
7. Click *OK*.
The group can now be used in identity based firewall policies.

To create an FSSO user group using imported FortiNAC groups and tags as members in the CLI:

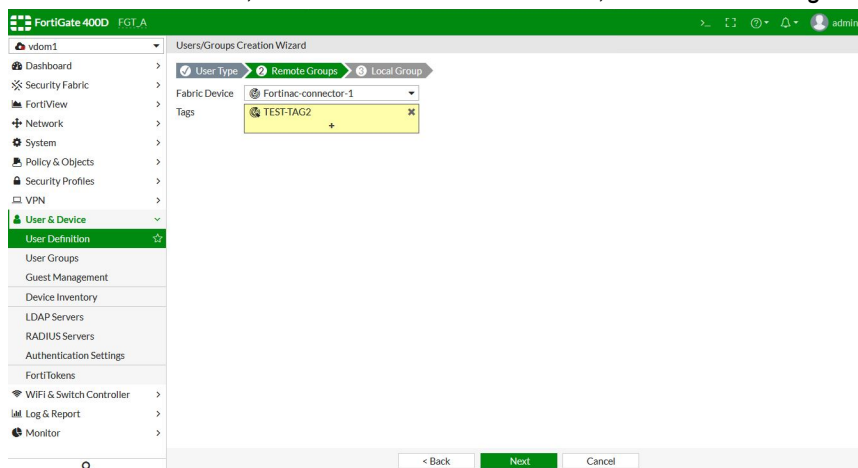
```
config user group
  edit "Fortinac-fsso-group"
    set group-type fsso-service
    set authtimeout 0
    set http-digest-realm ''
    set member "GROUP1" "GROUP2" "TEST-TAG1"
  next
end
```

To use the user/group creation wizard to create a new SSO group with the FortiNAC groups and firewall tags:

1. Go to *User & Device > User Definition* and click *Create New*.



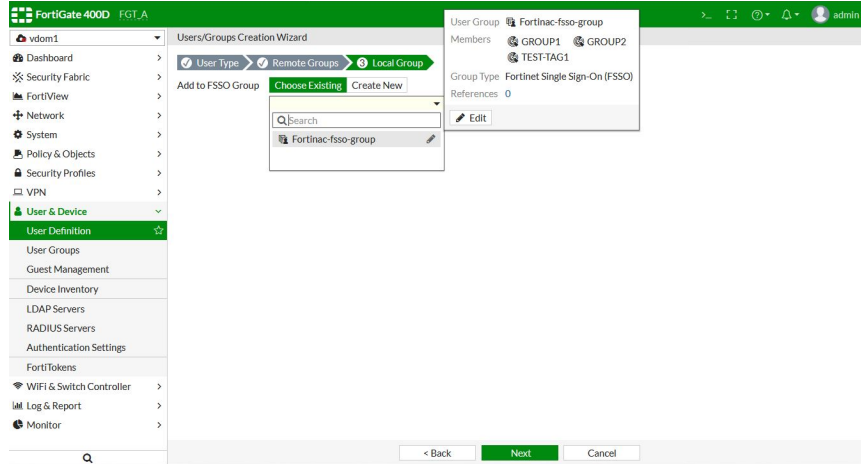
2. For the *User Type*, select *FortiNAC User*, then click *Next*.
3. For the *Fabric Device*, select the FortiNAC connector, then select the *Tags*.



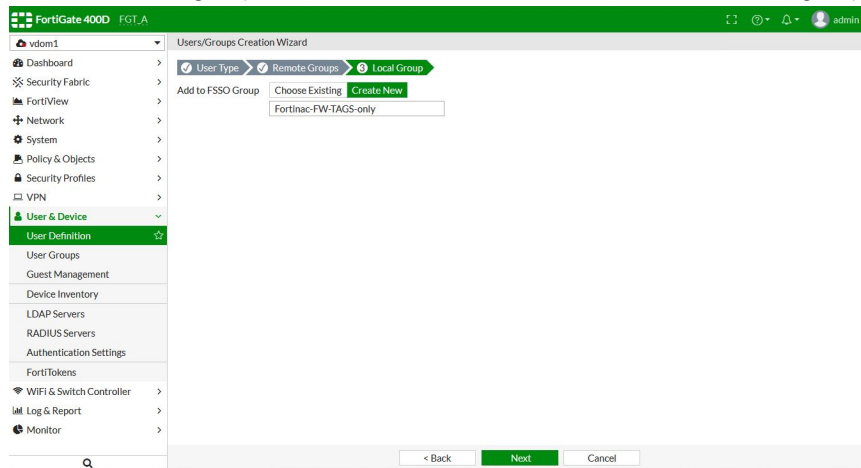
4. Click *Next*.

5. Either add the selected groups/tags to an existing SSO group, or create a new group:

- To add to an existing SSO group, click *Choose Existing*, and then select a group.

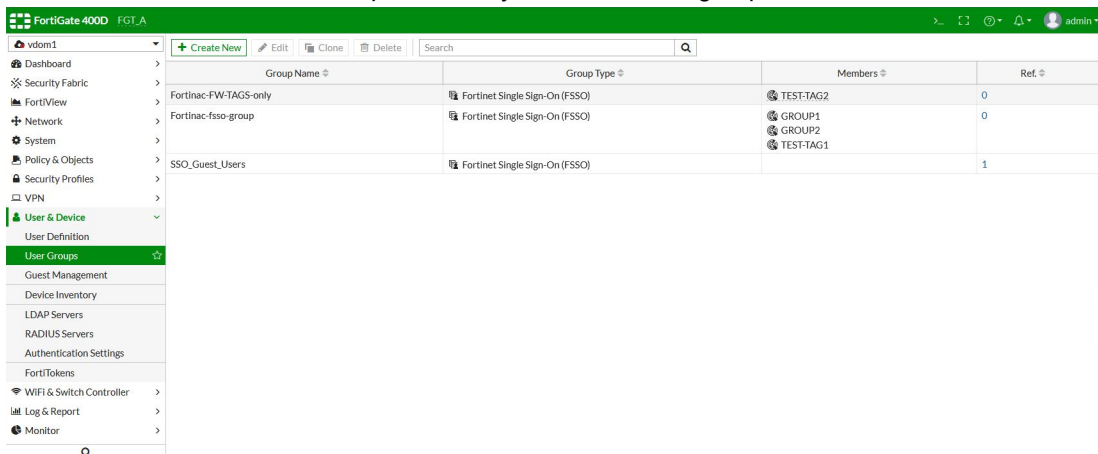


- To create a new group, click *Create New*, and then enter a name for the group.



6. Click *Next*.

7. Go to *User & Device > User Groups* and verify that the created groups are listed with the correct members.



Symantec endpoint connector

With the Fabric connector for Symantec Endpoint Protection Manager (SEPM), you can use the client IP information from SEPM to assign to dynamic IP addresses on FortiOS.

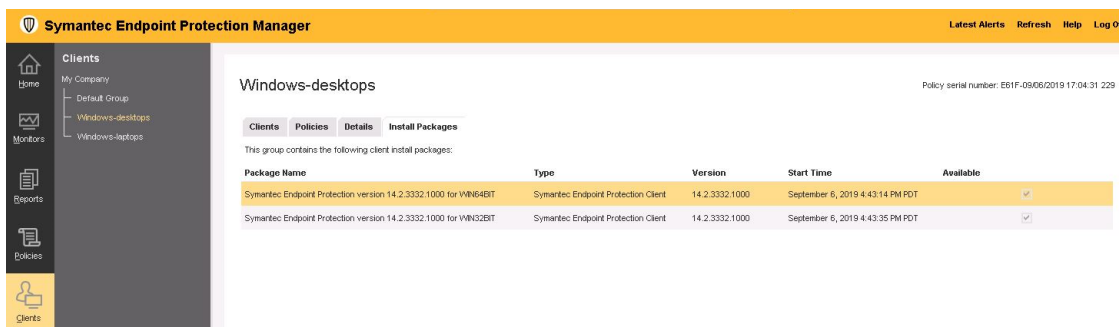
When communication between FortiGate and SEPM is established, FortiGate polls every minute for updates via TLS over port 8446. You can use the CLI to change the default one minute polling interval.

For example, you can create a dynamic Fabric Connector IP address subtype and use it in firewall policies as the source address. The dynamic IP address contains all IP addresses sent by SEPM.

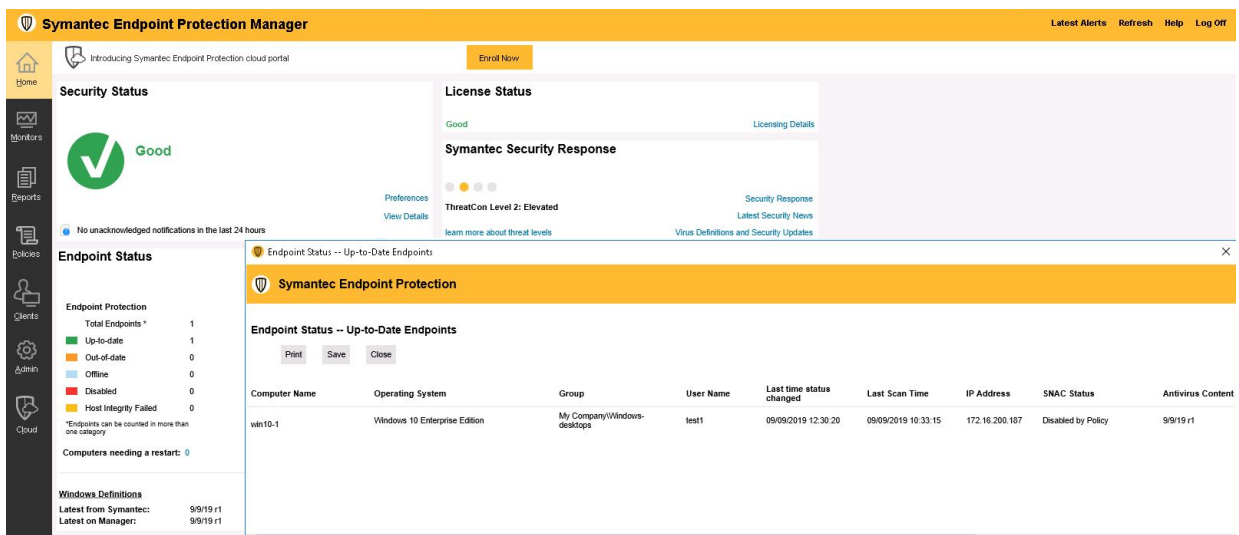
This example shows a dynamic IP address with SEPM and one client PC managed by SEPM using FortiGate as the default gateway.

To configure SEPM on a managed client PC:

1. In SEPM, create client packages for client hosts and group them into SEPM groups.
You can install packages locally on clients or download them directly from SEPM.

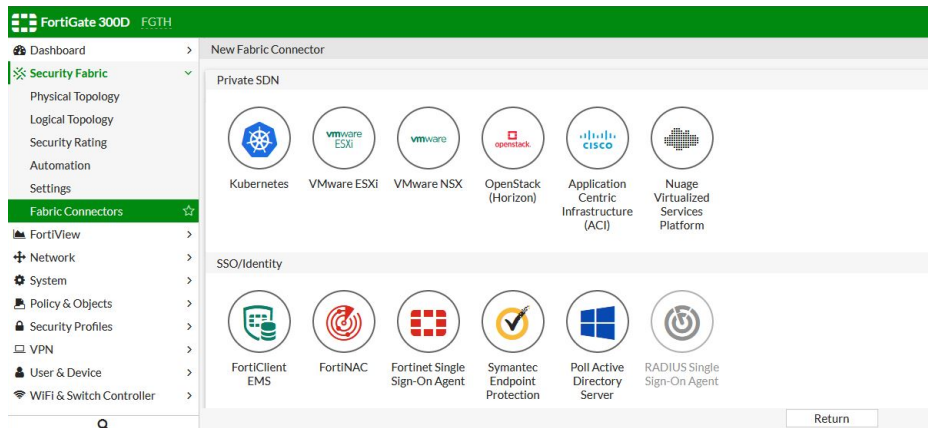


2. When a package is installed on the client host, the host is considered managed by SEPM.
Even if the host has multiple interfaces, only one IP per host is displayed.

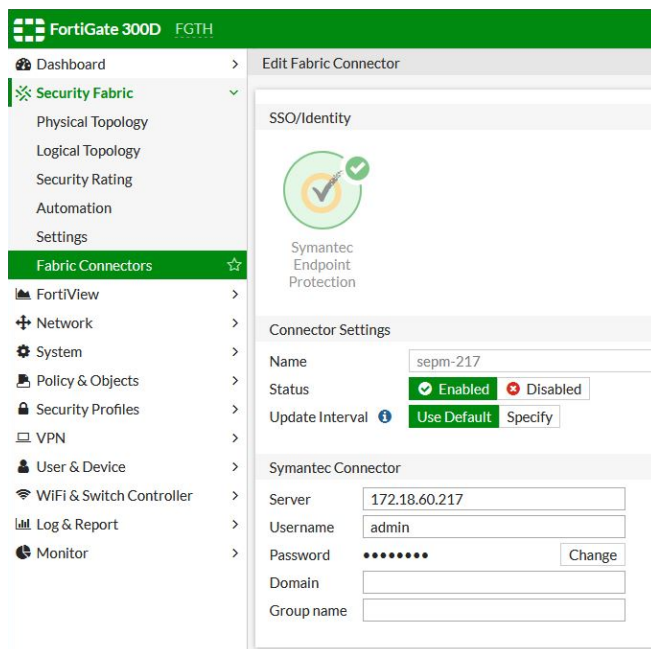


To configure Symantec endpoint connector on FortiGate in the GUI:

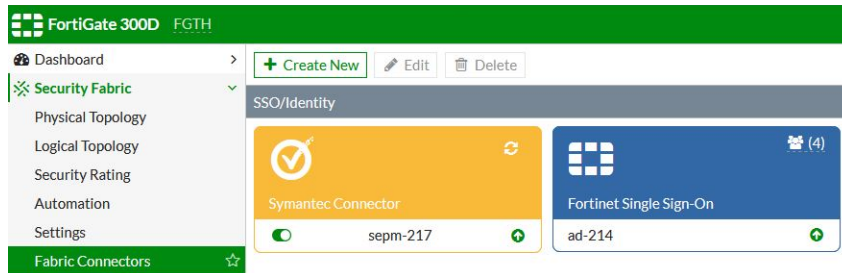
1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New*.



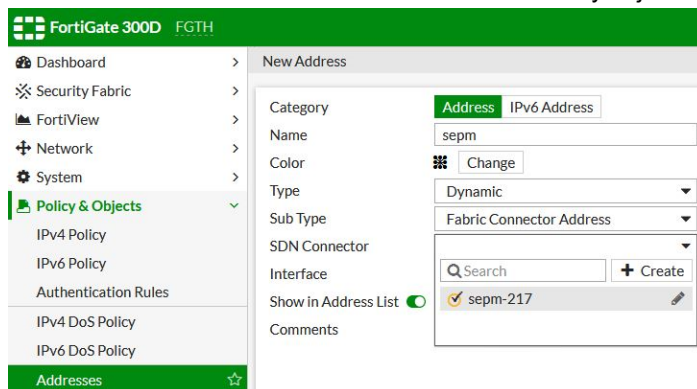
3. Click *Symantec Endpoint Protection*.
 - In the *Connector Settings* section, if options are left empty, then all SEPM domains and groups are monitored.
 - In the *Symantec Connector* section:
 - In the *Server* field, enter the SEPM IP address.
 - Enter the *Username* and *Password*.
 - If you want to limit the domains or groups that are monitored, enter the information in *Domain* and *Group name*.



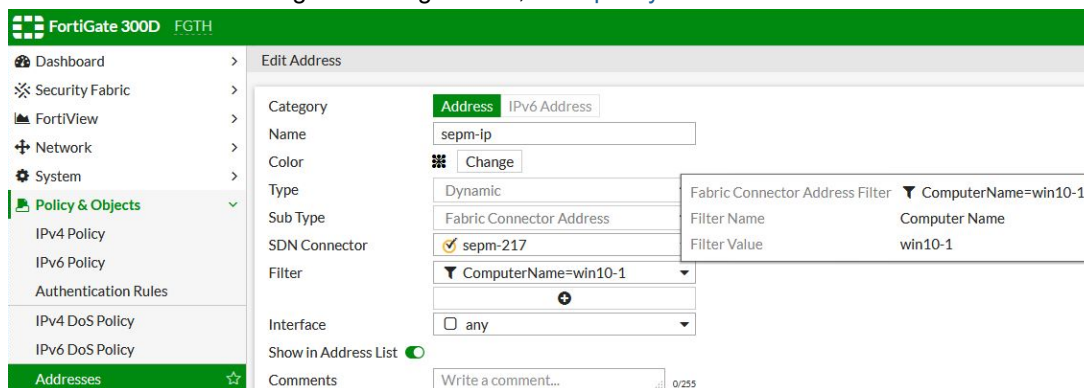
4. Click *OK*.
When the connection is established, you can see a green up arrow in the bottom right of the tile. You might need to refresh your browser to see the established connection.



5. Go to *Policy & Objects > Addresses*.
6. Click *Create New > Address*.
 - Set *Type* to *Dynamic*.
 - Set *Sub Type* to *Fabric Connector Address*.
 - Set *SDN Connector* to the Fabric Connector that you just created.



7. Click *OK*.
8. Edit the address to see the configuration.
 - *Filter* shows the hostnames of the client PCs managed by SEPM. The GUI shows the *ComputerName* by default. You can change this using the CLI; see [Specify filters](#) for details.



Filter options are only available for active computers that are configured and registered in SEPM. Free-form filters can be created manually by clicking *Create* and entering the filter, in the format: `filter_type=value`.

Possible manual filter types are: `GroupName`, `GroupID`, `ComputerName`, `ComputerUUID`, and `OSName`. For example: `GroupName=MyGroup`.

9. In *Policy & Objects* > *Addresses*, you can see all the IP addresses of the host.

Name	Type	Details	Interface	Visibility	Ref.
Address 12					
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	2
all	Subnet	0.0.0.0/0		Visible	1
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	0
login.sepm-ip resolves to:	FQDN	login.microsoftonline.com		Visible	1
login	FQDN	login.windows.net		Visible	0
none	Subnet	0.0.0.0/32		Visible	0
sepm-ip	Dynamic			Visible	1
wildcard.dropbox.com	FQDN	*dropbox.com		Visible	0
wildcard.google.com	FQDN	*google.com		Visible	0
Address Group 2					
IPv6 Address 3					

10. Go to *Policy & Objects* > *IPv4 Policy*, click *Create New* and add the dynamic IP address to the firewall policy.

Edit Policy

Name: pol1

Incoming Interface: port2

Outgoing Interface: port1

Source: sepm-ip

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT

Inspection Mode: Flow-based

Firewall / Network Options

NAT: ☒

IP Pool Configuration: Use Outgoing Interface Address

Preserve Source Port: ☐

Protocol Options: default

Security Profiles

AntiVirus: default

Web Filter: ☐

DNS Filter: ☐

Application Control: ☐

IPS: ☐

SSL Inspection: certificate-inspection

Select Entries

Address User Internet Service

Search

ADDRESS (10)

all

FABRIC_DEVICE

gmail.com

login.microsoft.com

login.microsoftonline.com

login.windows.net

none

sepm-ip

wildcard.dropbox.com

wildcard.google.com

ADDRESS GROUP (2)

G Suite

Microsoft Office 365

Close

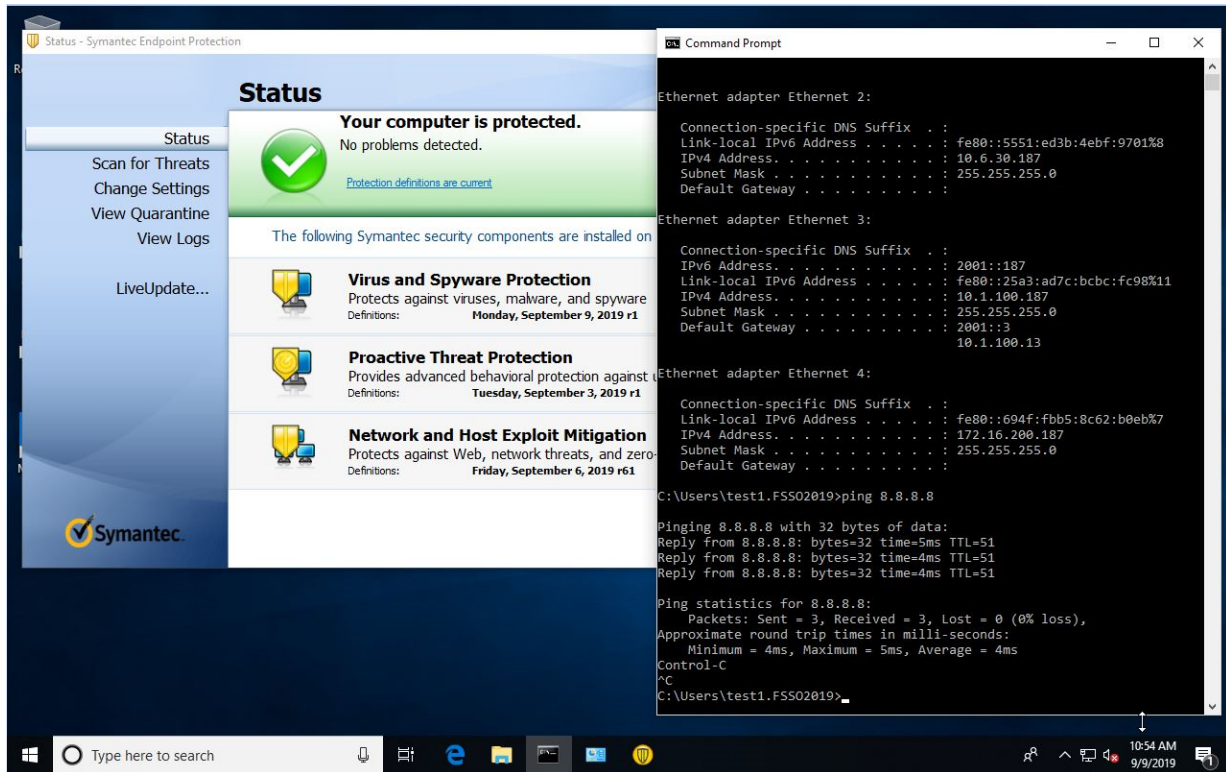
Documentation

Online Help

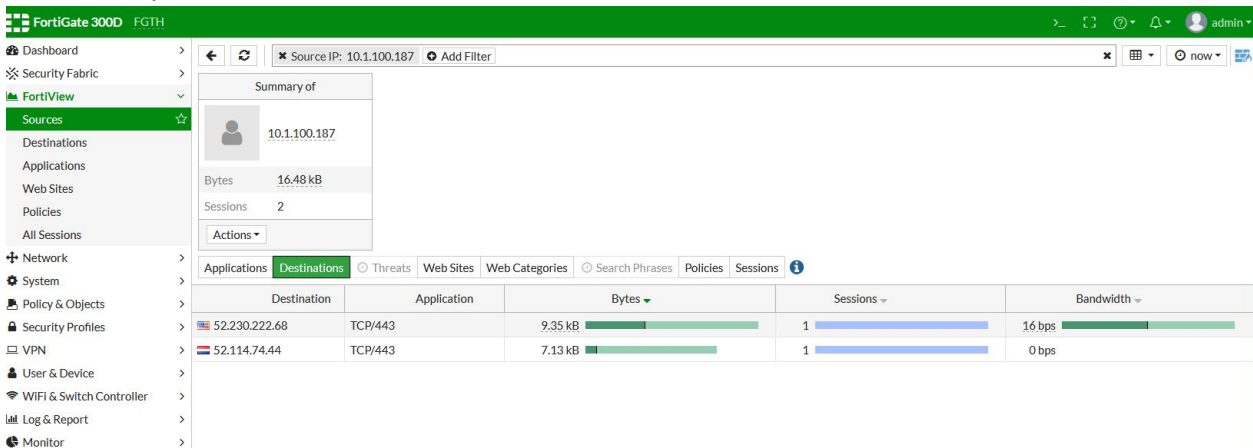
Video Tutorials

To verify the configuration:

1. On the client PC, check that it is managed by SEPM to access the Internet.



2. In FortiGate, you can check in *FortiView* > *Sources*.



3. In FortiGate, you can also check in *Log & Report > Forward Traffic*.

Date/Time	Source	Device	Destination	Application Name
2019/09/09 11:16:17	10.1.100.187	WIN10-1	13.32.253.39	
2019/09/09 11:11:17	10.1.100.187	WIN10-1	13.32.253.227	
2019/09/09 11:08:53	10.1.100.187	WIN10-1	23.60.73.11	
2019/09/09 11:08:53	10.1.100.187	WIN10-1	23.60.73.11	
2019/09/09 11:08:53	10.1.100.187	WIN10-1	23.195.226.49	
2019/09/09 11:08:53	10.1.100.187	WIN10-1	23.60.73.11	
2019/09/09 11:08:51	10.1.100.187	WIN10-1	23.60.73.11	
2019/09/09 11:08:51	10.1.100.187	WIN10-1	23.60.73.11	
2019/09/09 11:07:58	10.1.100.187	WIN10-1	216.58.217.46 (den03s10-in-f46.1e100.net)	
2019/09/09 11:07:57	10.1.100.187	WIN10-1	216.58.217.46 (den03s10-in-f46.1e100.net)	
2019/09/09 11:07:40	10.1.100.187	WIN10-1	52.114.77.34	
2019/09/09 11:06:55	10.1.100.187	WIN10-1	52.158.238.42	
2019/09/09 11:06:55	10.1.100.187	WIN10-1	13.68.92.143	
2019/09/09 11:06:53	10.1.100.187	WIN10-1	173.194.152.56	
2019/09/09 11:06:50	10.1.100.187	WIN10-1	173.194.152.75	
2019/09/09 11:06:38	10.1.100.187	WIN10-1	52.177.83.224	
2019/09/09 11:06:32	10.1.100.187	WIN10-1	216.58.217.35	
2019/09/09 11:06:28	10.1.100.187	WIN10-1	173.194.152.87	
2019/09/09 11:06:23	10.1.100.187	WIN10-1	173.194.152.88	
2019/09/09 11:06:23	10.1.100.187	WIN10-1	209.52.146.51	
2019/09/09 11:06:23	10.1.100.187	WIN10-1	173.194.152.88	
2019/09/09 11:06:23	10.1.100.187	WIN10-1	209.52.146.51	
2019/09/09 11:06:22	10.1.100.187	WIN10-1	13.32.253.218 (server-13-32-253-218.sea19r.cloudfront.net)	
2019/09/09 11:06:20	10.1.100.187	WIN10-1	173.194.152.58	



Since this traffic is not authenticated traffic but is based on source IP address only, this traffic is not shown in the GUI firewall monitor or in the CLI `diagnose firewall auth list` command.

To configure Symantec endpoint connector on FortiGate in the CLI:

1. Create the fabric connector:

```
config system sdn-connector
  edit "sepm-217"
    set type sepm
    set server "172.18.60.217"
    set username "admin"
    set password "*****"
    set status enable
  next
end
```

2. Create the dynamic IP address:

```
config firewall address
  edit "sepm-ip"
    set uuid 645552a0-d0c9-51e9-282d-c7ed6d7ee7de
    set type dynamic
    set sdn "sepm-217"
    set filter "ComputerName=win10-1"
  config list
    edit "10.1.100.187"
```

```

        next
        edit "10.6.30.187"
        next
        edit "172.16.200.187"
        next
    end
next
end

```

You can specify other filters and combine them with | and &, for example:

```

FGTH (sepm-ip) # set filter
<key1=value1>    [& <key2=value2>] [| <key3=value3>]
Available filter keys are:
    <ComputerName><ComputerUuid><GroupId><GroupName> <DomainId><DomainName><OsName>

```

3. Add the dynamic IP address to the firewall policy:

```

config firewall policy
    edit 1
        set name "pol1"
        set uuid 9174563c-d0c9-51e9-1a32-4e14385239e9
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "sepm-ip"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
        set logtraffic all
        set fsso disable
        set nat enable
    next
end

```

To troubleshoot Symantec SD connector in the CLI:

```
# diagnose debug application sepm -1
```

Output is sent every minute (default). All IPv4 learned from SEPM. IPv6 also sent but not yet supported.

```

2019-09-09 12:01:09 sepm sdn connector sepm-217 start updating IP addresses
2019-09-09 12:01:09 sepm checking firewall address object sepm-ip, vd 0
2019-09-09 12:01:09 sepm sdn connector sepm-217 finish updating IP addresses
2019-09-09 12:01:09 sepm reap child pid: 18079
2019-09-09 12:02:09 sepm sdn connector sepm-217 prepare to update
2019-09-09 12:02:09 sepm sdn connector sepm-217 start updating
2019-09-09 12:02:09 sepm-217 sdn connector will retrieve token after 9526 secs
2019-09-09 12:02:09 sym_new_ip_addr ComputerName win10-1
    ComputerUuid AC894D56-BD86-A786-7DDB-7FD98B718AE0, OsName Windows 10
    IP 172.16.200.187
    GroupName My Company\Windows-desktops, GroupId E61FDEA2AC10C80E46D0B31BB58D7CB3
    DomainName Default, DomainId 6C507580AC10C80E5F3CAED5B1711A8E
2019-09-09 12:02:09 sym_new_ip_addr ComputerName win10-1

```

```

ComputerUuid AC894D56-BD86-A786-7DDB-7FD98B718AE0, OsName Windows 10
IP 10.6.30.187
GroupName My Company\Windows-desktops, GroupId E61FDEA2AC10C80E46D0B31BB58D7CB3
DomainName Default, DomainId 6C507580AC10C80E5F3CAED5B1711A8E
2019-09-09 12:02:09 sym_new_ip_addr ComputerName win10-1
ComputerUuid AC894D56-BD86-A786-7DDB-7FD98B718AE0, OsName Windows 10
IP 10.1.100.187
GroupName My Company\Windows-desktops, GroupId E61FDEA2AC10C80E46D0B31BB58D7CB3
DomainName Default, DomainId 6C507580AC10C80E5F3CAED5B1711A8E
2019-09-09 12:02:09 2001:0000:0000:0000:0000:0000:0000:0187 is not in IPv4 presentation
format

2019-09-09 12:02:09 sepmd sdn connector sepm-217 start updating IP addresses
2019-09-09 12:02:09 sepmd checking firewall address object sepm-ip, vd 0
2019-09-09 12:02:09 sepmd sdn connector sepm-217 finish updating IP addresses
2019-09-09 12:02:09 sepmd reap child pid: 18089
2019-09-09 12:03:09 sepmd sdn connector sepm-217 prepare to update
2019-09-09 12:03:09 sepmd sdn connector sepm-217 start updating
2019-09-09 12:03:09 sepm-217 sdn connector will retrieve token after 9466 secs
2019-09-09 12:03:09 sym_new_ip_addr ComputerName win10-1
ComputerUuid AC894D56-BD86-A786-7DDB-7FD98B718AE0, OsName Windows 10
IP 172.16.200.187
GroupName My Company\Windows-desktops, GroupId E61FDEA2AC10C80E46D0B31BB58D7CB3
DomainName Default, DomainId 6C507580AC10C80E5F3CAED5B1711A8E
2019-09-09 12:03:09 sym_new_ip_addr ComputerName win10-1
ComputerUuid AC894D56-BD86-A786-7DDB-7FD98B718AE0, OsName Windows 10
IP 10.6.30.187
GroupName My Company\Windows-desktops, GroupId E61FDEA2AC10C80E46D0B31BB58D7CB3
DomainName Default, DomainId 6C507580AC10C80E5F3CAED5B1711A8E
2019-09-09 12:03:09 sym_new_ip_addr ComputerName win10-1
ComputerUuid AC894D56-BD86-A786-7DDB-7FD98B718AE0, OsName Windows 10
IP 10.1.100.187
GroupName My Company\Windows-desktops, GroupId E61FDEA2AC10C80E46D0B31BB58D7CB3
DomainName Default, DomainId 6C507580AC10C80E5F3CAED5B1711A8E
2019-09-09 12:03:09 2001:0000:0000:0000:0000:0000:0000:0187 is not in IPv4 presentation
format

```

To list the SEPM daemon SDN connectors:

```

diagnose test application sepmd 1
sepm SDN connector list:
  name: sepm-217, status: enabled, updater_interval: 60

```

To list the SEPM daemon SDN filters:

```

diagnose test application sepmd 2
sepm SDN connector sepm-217 filter list:
  name: sepm-ip, vd 0, filter 'ComputerName=win10-1'

```

RADIUS single sign-on (RSSO) agent

With RSSO, a FortiGate can authenticate users who have authenticated on a remote RADIUS server. Based on which user group the user belongs to, the security policy applies the appropriate UTM profiles.

The FortiGate does not interact with the remote RADIUS server; it only monitors RADIUS accounting records that the server forwards (originating from the RADIUS client). These records include the user IP address and user group. The remote RADIUS server sends the following accounting messages to the FortiGate:

Message	Action
Start	If the information in the start message matches the RSSO configuration on the FortiGate, the user is added to the local list of authenticated firewall users.
Stop	The user is removed from the local list of authenticated firewall users because the user session no longer exists on the RADIUS server.

You can configure an RSSO agent connector using the FortiOS GUI; however, in most cases, you will need to use the CLI. There are some default options you may need to modify, which can only be done in the CLI.

To configure an RSSO agent connector:

1. Create the new connector:
 - a. Go to *Security Fabric > Fabric Connectors*.
 - b. Click *Create New*.
 - c. In the *SSO/Identity* section, click *RADIUS Single Sign-On Agent*. The *New Fabric Connector* pane opens.
 - d. Enter the connector name.
 - e. Enable *Use RADIUS Shared Secret*.



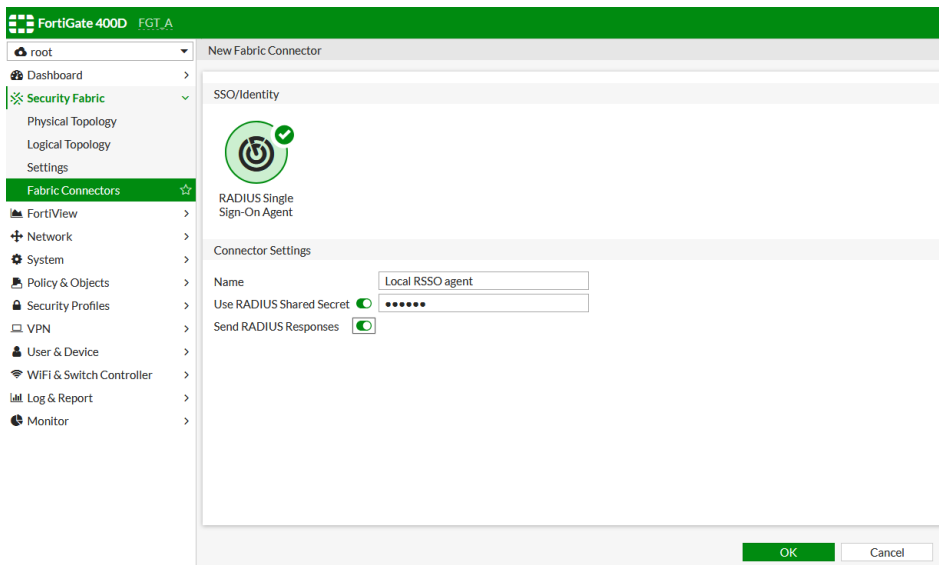
The value entered in *Use RADIUS Shared Secret* must be identical to what the remote RADIUS server uses to authenticate when it sends RADIUS accounting messages to the FortiGate.

- f. Enable *Send RADIUS Responses*.



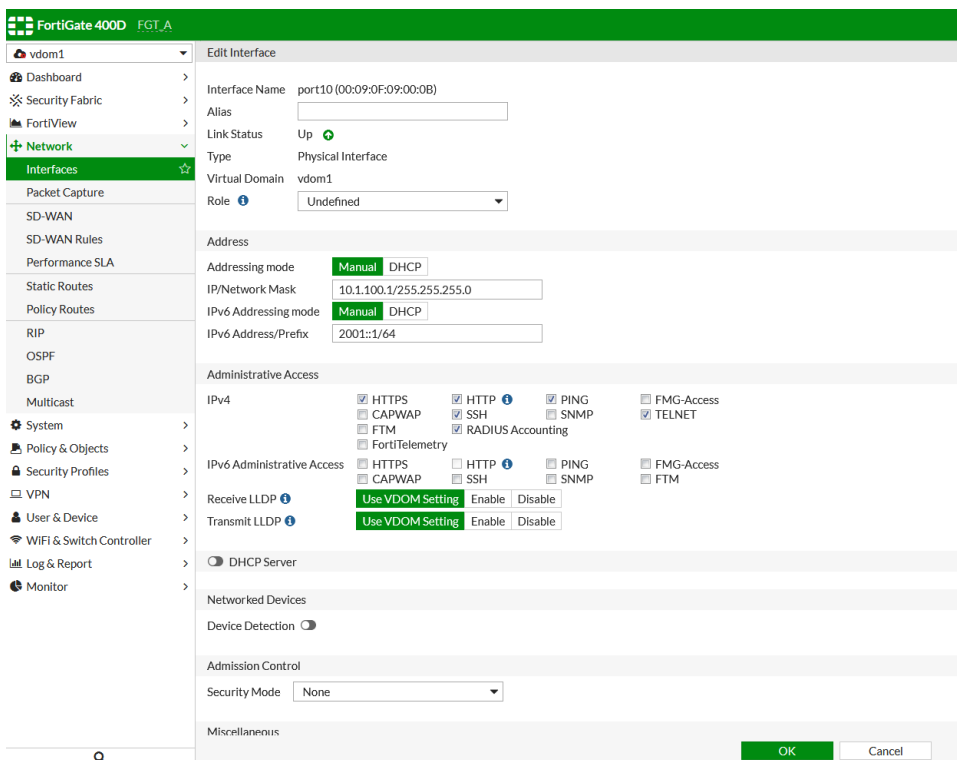
You should enable *Send RADIUS Responses* because some RADIUS servers continue to send the same RADIUS accounting message several times if there is no response.

g. Click OK.



2. Edit the network interface:

- a. Go to *Network > Interfaces*.
- b. Double-click the interface that will receive the RADIUS accounting messages. The *Edit Interface* pane opens.
- c. In the *Administrative Access* section, select the *RADIUS Accounting* checkbox. This will open listening for port 1813 on this interface. The FortiGate will then be ready to receive RADIUS accounting messages.
- d. Click OK.



3. Create a local RSSO user group:

- a. Go to *User & Device > User Groups*.
- b. Click *Create New*.

- c. Enter the group name.
- d. For the *Type* field, click *RADIUS Single-Sign-ON (RSSO)*.
- e. Enter a value for *RADIUS Attribute Value*.

This value by default is the class attribute. The FortiGate uses the content of this attribute in RADIUS accounting start messages to map a user to a FortiGate group, which then can be used in firewall policies.

In this example configuration, the FortiGate will only add a remote RADIUS user to the local firewall user list if the class attribute in the RADIUS accounting START message contains the value group1.



If your users are in multiple groups, you will need to add another local RSSO user group.



If the RADIUS attribute value used to map users to a local RSSO group is different than the RADIUS attribute in the RADIUS accounting messages forwarded by the server, you must change it in the CLI.

- f. Click OK.

The screenshot shows the FortiGate 400D FGT_A web interface. On the left is a navigation menu with options like Dashboard, Security Fabric, FortiView, Network, System, Policy & Objects, Security Profiles, VPN, User & Device, User Definition, User Groups, Guest Management, Device Inventory, LDAP Servers, RADIUS Servers, Authentication Settings, FortiTokens, WiFi & Switch Controller, Log & Report, and Monitor. The 'User & Device' section is expanded, and 'User Groups' is selected. The main area shows the 'New User Group' configuration form. The 'Name' field contains 'rso-group-1'. The 'Type' dropdown menu is open, showing options: Firewall, Fortinet Single Sign-On (FSSO), RADIUS Single Sign-On (RSSO) (which is highlighted), and Guest. The 'RADIUS Attribute Value' field contains 'group1'. At the bottom right of the form are 'OK' and 'Cancel' buttons.

- 4. Edit the local RSSO agent to modify default options using the CLI.

For example, the default value for `rsso-endpoint-attribute` might work in common remote access scenarios where users are identified by their unique `Calling-Station-Id`, but in other scenarios the user name might be in a different attribute.

```
config user radius
  edit "Local RSSO Agent"
    set rsso-endpoint-attribute <attribute>
    set sso-attribute <attribute>
  next
end
```

- 5. Add the local RSSO user group to a firewall policy.

Verifying the RSSO configuration

Verification requires a working remote RADIUS server configured for RADIUS accounting forwarding and wireless or wired clients that use RADIUS for user authentication.

For a quick test, you can use one of the publicly available RADIUS test tools to send RADIUS accounting start and stop messages to the FortiGate. You can also use [radclient](#).

To verify the RSSO configuration:

1. In radclient, enter the RADIUS attributes. These attributes are then executed with the FortiGate IP parameters (sends accounting messages to port 1813) and shared password you configured. -x is used for verbose output:

```
root@ControlPC:~# echo "Acct-Status-Type =Start,Framed-Ip-Address=10.1.100.185,User-
Name=test2,Acct-Session-Id=0211a4ef,Class=group1,Calling-Station-Id=00-0c-29-44-BE-B8" |
radclient -x 10.1.100.1 acct 123456
Sending Accounting-Request of id 180 to 10.1.100.1 port 1813
  Acct-Status-Type = Start
  Framed-IP-Address = 10.1.100.185
  User-Name = "test2"
  Acct-Session-Id = "0211a4ef"
  Class = 0x67726f757031
  Calling-Station-Id = "00-0c-29-44-BE-B8"
rad_recv: Accounting-Response packet from host 10.1.100.1 port 1813, id=180, length=20
root@ControlPC:~#
```

2. Verify that the user is in the local firewall user list with the correct type (rsso) and local firewall group (rsso-group1):

```
# diagnose firewall auth 1

10.1.100.185, test2
  type: rsso, id: 0, duration: 5, idled: 5
  flag(10): radius
  server: vdom1
  packets: in 0 out 0, bytes: in 0 out 0
  group_id: 3
  group_name: rsso-group-1

----- 1 listed, 0 filtered -----
```

Threat feeds

Threat feeds dynamically import an external block lists from an HTTP server in the form of a plain text file. Block lists can be used to enforce special security requirements, such as long term policies to always block access to certain websites, or short term requirements to block access to known compromised locations. The lists are dynamically imported, so that any changes are immediately imported by FortiOS.

There are four types of threat feeds:

FortiGuard Category	The file contains one URL per line. It is available as a <i>Remote Category</i> in Web Filter profiles and SSL inspection exemptions. Example:
----------------------------	---


```
http://example.com.url
https://example.com/url
http://example.com:8080/url
```

IP Address The file contains one IP/IP range/subnet per line. It is available as an *External IP Block List* in DNS Filter profiles, and as a *Source/Destination* in IPv4, IPv6, and proxy policies.

Example:

```
192.168.2.100
172.200.1.4/16
172.16.1.2/24
172.16.8.1-172.16.8.100
2001:0db8::eade:27ff:fe04:9a01/120
2001:0db8::eade:27ff:fe04:aa01-2001:0db8::eade:27ff:fe04:ab01
```

Domain Name The file contains one domain per line. Simple wildcards are supported. It is available as a *Remote Category* in DNS Filter profiles. See [External resources for DNS filter on page 228](#).

Example:

```
mail.*.example.com
*-special.example.com
www.*example.com
example.com
```

Malware Hash The file contains one hash per line in the format <hex hash> [optional hash description]. Each line supports MD5, SHA1, and SHA256 hex hashes. It is automatically used for virus outbreak prevention on antivirus profiles with `external-blocklist` enabled.

Note: For optimal performance, do not mix different hashes in the list. Only use one of MD5, SHA1, or SHA26.

Example:

```
292b2e6bb027cd4ff4d24e338f5c48de
dda37961870ce079defbf185eeef905 Trojan-Ransom.Win32.Locky.abfl
3fa86717650a17d075d856a41b3874265f8e9eab Trojan-Ransom.Win32.Locky.abfl
c35f705df9e475305c0984b05991d444450809c35dd1d96106bb8e7128b9082f
Trojan-Ransom.Win32.Locky.abfl
```

See [External malware block list for antivirus on page 913](#) for an example.

External resources file format

File format requirements for an external resources file:

- The file is in plain text format with each URL list, IP address, and domain name occupying one line.
- The file is limited to 10 MB or 128 × 1024 (131072) entries, whichever limit is hit first.
- The entry limit also follows the table size limitation defined by CMDDB per model.
- The external resources update period can be set to 1 minute, hourly, daily, weekly, or monthly (43200 min, 30 days).
- The external resources type as category (URL list) and domain (domain name list) share the category number range 192 to 221 (total of 30 categories).
- There is no duplicated entry validation for the external resources file (entry inside each file or inside different files).
- If the number of entries exceed the limit, a warning is displayed. Additional entries beyond the threshold will not be loaded.

For domain name list (type = domain):

- Simple wildcards are allowed in the domain name list, for example: *.test.com.
- IDN (international domain name) is supported.

For IP address list (type = address):

- The IP address can be a single IP address, subnet address, or address range. For example, 192.168.1.1, 192.168.10.0/24, or 192.168.100.1-192.168.100.254.
- The address can be an IPv4 or IPv6 address. An IPv6 address does not need to be in [] format.

To determine the external resource table size limit for your device:

```
# print tablesize
...
system.external-resource: 0 256 512
...
```

For this device, a FortiGate 60E, the global limit is 512 and the limit per VDOM is 256.

Create a threat feed

To create a threat feed in the GUI:

1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New*.
3. In the *Thread Feeds* section, click on the required feed type.
4. Configure the connector settings:

Name	Enter a name for the threat feed connector.
URI of external resource	Enter the link to the external resource file. The file should be a plain text file with one entry on each line.
HTTP basic authentication	Enable/disable basic HTTP authentication. When enabled, enter the username and password in the requisite fields.
Refresh Rate	The time interval to refresh the external resource, in minutes (1 - 43200, default = 5).
Comments	Optionally, enter a description of the connector.
Status	Enable/disable the connector.

5. Click *OK*.

To create a threat feed in the CLI:

```
config system external-resource
  edit <name>
    set status {enable | disable}
    set type {category | address | domain | malware}
    set category <integer>
    set username <string>
    set password <string>
    set comments [comments]
    *set resource <resource-uri>
```

```

    *set refresh-rate <integer>
    set source-ip <string>
next
end

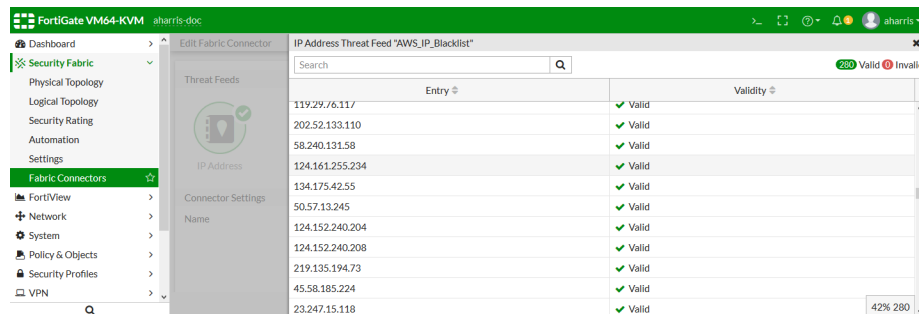
```

Parameters marked with a * are mandatory and must be filled in. Other parameters either have default values or are optional.

Update history

To review the update history of a threat feed, go to *Security Fabric > Fabric Connectors*, select a feed, and click *Edit*. The *Last Update* field shows the date and time that the feed was last updated.

Click *View Entries* to view the current entries in the list.



Entry	Validity
119.29.76.117	Valid
202.52.133.110	Valid
58.240.131.58	Valid
124.161.255.234	Valid
134.175.42.55	Valid
50.57.13.245	Valid
124.152.240.204	Valid
124.152.240.208	Valid
219.135.194.73	Valid
45.58.185.224	Valid
23.247.15.118	Valid

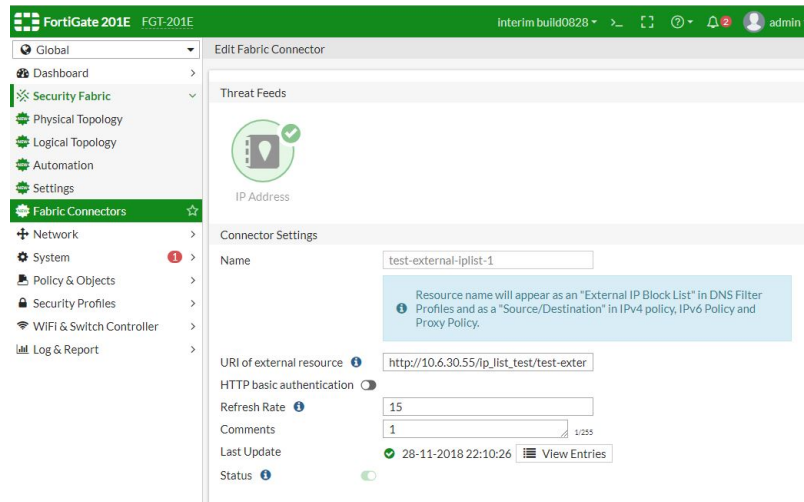
42% 280

External Block List (Threat Feed) – Policy

You can use the External Block List (Threat Feed) for web filtering and DNS. You can also use External Block List (Threat Feed) in firewall policies.

Sample configuration

In *Security Fabric > Fabric Connectors > Threat Feeds > IP Address*, create or edit an external IP list object.



Threat Feeds

IP Address

Connector Settings

Name: test-external-ip-list-1

URI of external resource: http://10.6.30.55/ip_list_test/test-exter

HTTP basic authentication: ☐

Refresh Rate: 15

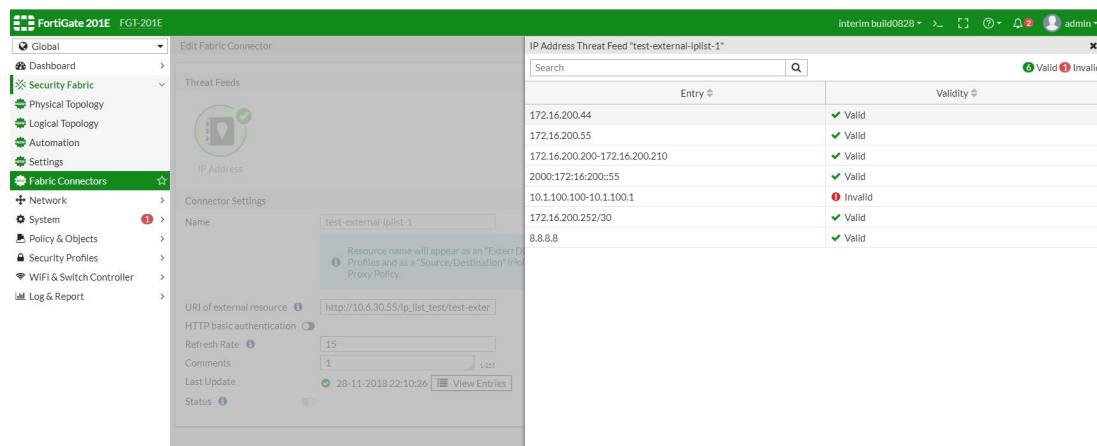
Comments: 1

Last Update: 28-11-2018 22:10:26

Status: ☒ Valid

[View Entries](#)

Click *View Entries* to see the external IP list.



To create an external iplist object using the CLI:

```
config system external-resource
edit "test-external-iplist-1"
set status enable
set type address
set username ''
set password ENC
set comments ''
set resource "http://10.6.30.55/ip_list_test/test-external-iplist-2.txt"
set refresh-rate 15
next
end
```

To apply an external iplist object to the firewall policy using the CLI:

```
config firewall policy
edit 1
set name "policyid-1"
set srcintf "wan2"
set dstintf "wan1"
set srcaddr "all"
set dstaddr "test-external-iplist-1"
set action accept
set schedule "always"
set service "ALL"
set logtraffic all
set auto-asic-offload disable
set nat enable
next
end
```

External Block List (Threat Feed) - Authentication

The external *Threat Feed* connector (block list retrieved by HTTPS) supports username and password authentication.

To enable username and password authentication:

1. Navigate to *Security Fabric > Fabric Connectors*.
2. Edit an existing *Threat Feed* or create a new one by selecting *Create New*.
3. In *Connector Settings*, select the *HTTP basic authentication* toggle to enable the feature.
4. Enter a username and password.

FortiGate 600D FGT600D-DNS-NAT

Global

Dashboard

Security Fabric

Physical Topology

Logical Topology

Automation

Settings

Fabric Connectors

Network

System

Policy & Objects

Security Profiles

WiFi & Switch Controller

Log & Report

New Fabric Connector

Threat Feeds

FortiGuard Category

Connector Settings

Name Remote-Category-1

URI of external resource [https://172.16.200.66/external-resourc](#)

HTTP basic authentication ☒

Username external

Password

Refresh Rate 5

Comments 0/255

Status ☒

Resource name will appear as a "Remote Category" in Web Filter Profiles and SSL inspection exemptions.

OK Cancel

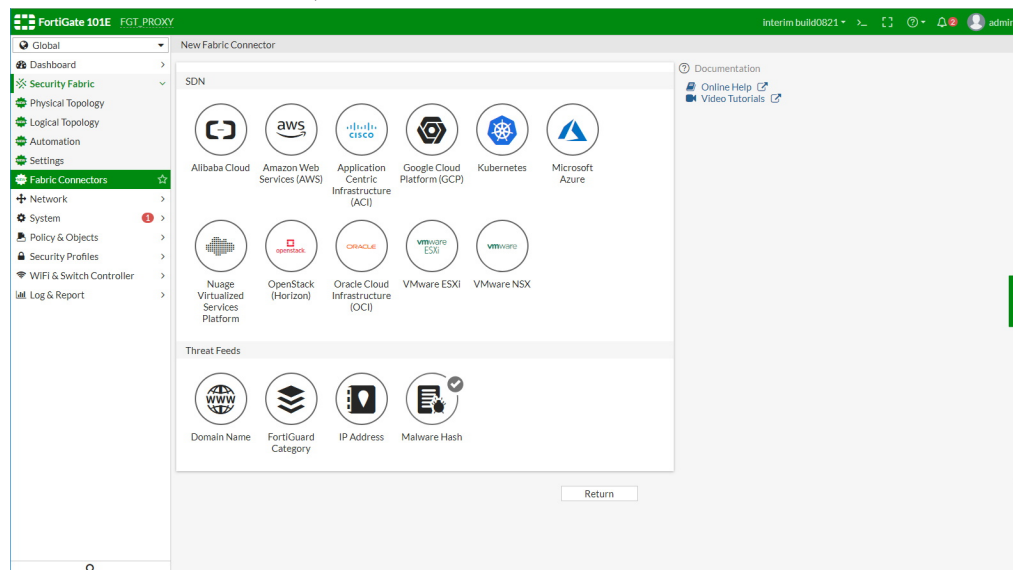
5. Select *OK* to save your changes.

External Block List (Threat Feed) - File Hashes

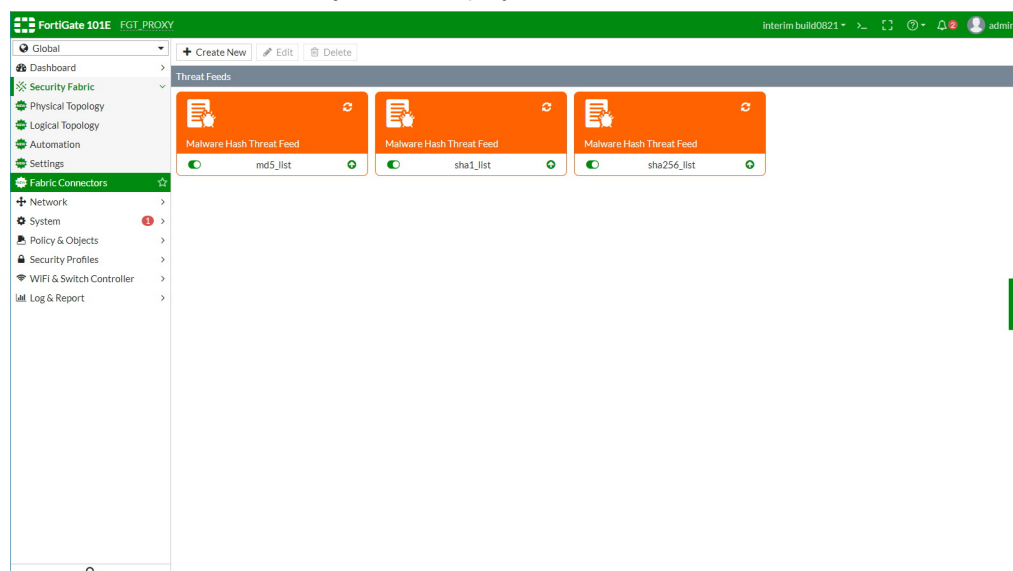
The Malware Hash type of *Threat Feed* connector supports a list of file hashes that can be used as part of virus outbreak prevention.

To configure Malware Hash:

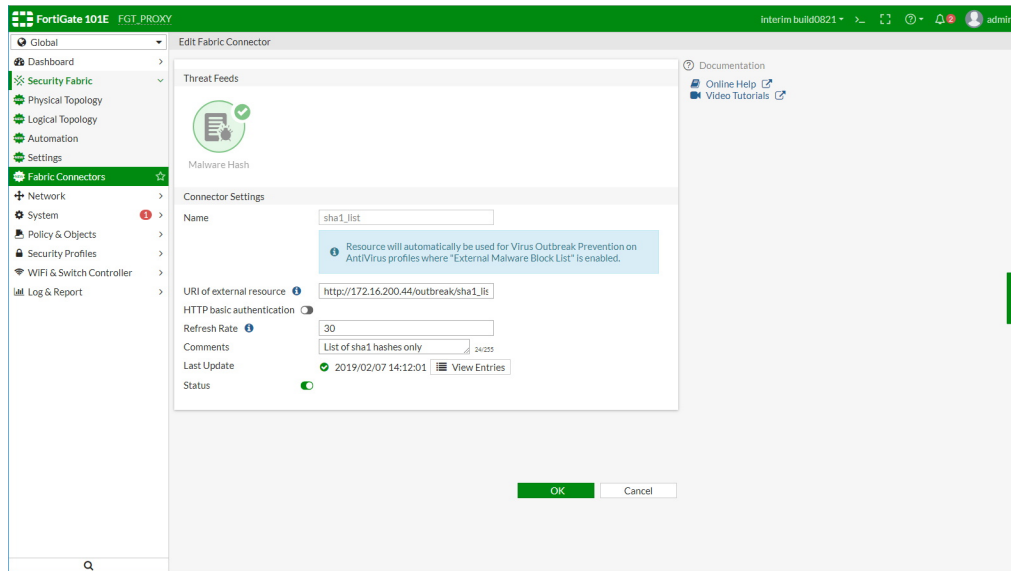
1. Navigate to *Security Fabric > Fabric Connectors* and click *Create New*.
2. In the *Threat Feeds* section, click *Malware Hash*.



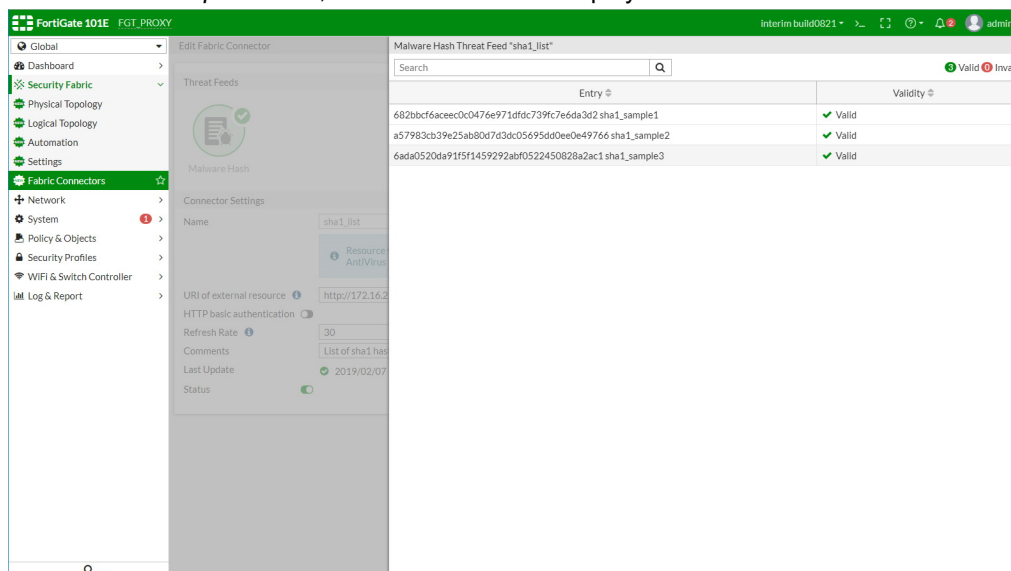
The *Malware Hash* source objects are displayed.



3. To configure *Malware Hash*, fill in the *Connector Settings* section.



4. Beside the *Last Update* field, click *View Entries* to display the external Malware Hash list contents.



New Malware value for external-resource parameter in CLI

```
FGT_PROXY (external-resource) # edit sha1_list
new entry 'sha1_list' added
```

```
FGT_PROXY (sha1_list) # set type ?
category      FortiGuard category.
address       Firewall IP address.
domain        Domain Name.
malware       Malware hash.
```

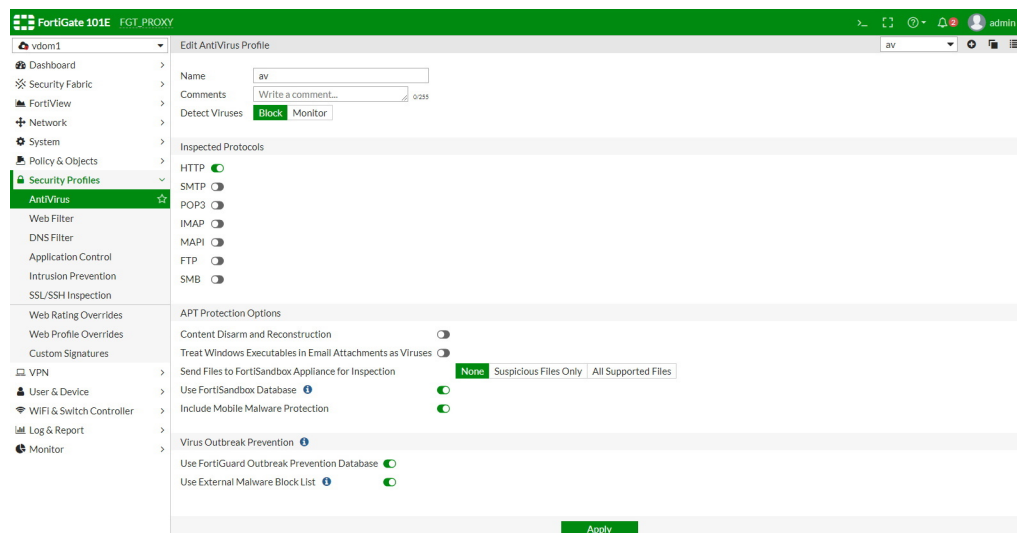
To configure external Malware Hash list sources in CLI:

```
config global
  config system external-resource
    edit "md5_list"
      set type malware
      set comments "List of md5 hashes only"
      set resource "http://172.16.200.44/outbreak/md5_list"
      set refresh-rate 30
    next
    edit "sha1_list"
      set type malware
      set comments "List of sha1 hashes only"
      set resource "http://172.16.200.44/outbreak/sha1_list"
      set refresh-rate 30
    next
    edit "sha256_list"
      set type malware
      set comments "List of sha256 hashes only"
      set resource "http://172.16.200.44/outbreak/sha256_list"
      set refresh-rate 30
    next
  end
end
```

Update to antivirus profile

In *Security Profiles > AntiVirus*, the *Virus Outbreak Prevention* section allows you to enable the following options:

- Use Fortinet outbreak Prevention Database.
- Use External Malware Block List.



To configure virus outbreak prevention options in CLI:

You must first enable outbreak-prevention in the protocol and then enable external-blocklist under outbreak-prevention.


```
config antivirus profile
  edit "av"
    set analytics-db enable
    config http
      set options scan
      set outbreak-prevention full-archive
    end
    config ftp
      set options scan
      set outbreak-prevention files
    end
    config imap
      set options scan
      set outbreak-prevention full-archive
    end
    config pop3
      set options scan
      set outbreak-prevention full-archive
    end
    config smtp
      set options scan
      set outbreak-prevention files
    end
    config mapi
      set options scan
      set outbreak-prevention full-archive
    end
    config nntp
      set options scan
      set outbreak-prevention full-archive
    end
    config smb
      set options scan
      set outbreak-prevention full-archive
    end
    config outbreak-prevention
      set ftgd-service enable
      set external-blocklist enable
    end
  next
end
```

Update to utm-virus category logs

This feature adds the fields `filehash` and `filehashsrc` to outbreak prevention detection events.

Example of the utm-virus log generated when a file is detected by FortiGuard queried outbreak prevention:

```
2: date=2018-07-30 time=13:57:59 logid="0204008202" type="utm" subtype="virus"
eventtype="outbreak-prevention" level="warning" vd="root" evnttime=1532984279 msg="Blocked
by Virus Outbreak Prevention service." action="blocked" service="HTTP" sessionid=174777
srcip=192.168.101.20 dstip=172.16.67.148 srcport=37044 dstport=80 srcintf="lan"
srcintfrole="lan" dstintf="wan1" dstintfrole="wan" policyid=1 proto=6 direction="incoming"
filename="zhvo_test.com" checksum="583369a5" quarskip="No-skip"
virus="503e99fe40ee120c45bc9a30835e7256fff3e46a" dtype="File Hash"
filehash="503e99fe40ee120c45bc9a30835e7256fff3e46a" filehashsrc="fortiguard"
```

```
url="http://172.16.67.148/zhvo_test.com" profile="mhash_test" agent="Firefox/43.0"
analyticssubmit="false" crscore=30 crlevel="high&#8220;
```

Example of the utm-virus log generated when a file is detected by External Malware Hash List outbreak prevention:

```
1: date=2018-07-30 time=13:59:41 logid="0207008212" type="utm" subtype="virus"
eventtype="malware-list" level="warning" vd="root" eventtime=1532984381 msg="Blocked by
local malware list." action="blocked" service="HTTP" sessionid=174963 srcip=192.168.101.20
dstip=172.16.67.148 srcport=37045 dstport=80 srcintf="lan" srcintfrole="lan" dstintf="wan1"
dstintfrole="wan" policyid=1 proto=6 direction="incoming" filename="mhash_block.com"
checksum="90f0cb57" quarskip="No-skip" virus="mhash_block.com" dtype="File Hash"
filehash="93bdd30bd381b018b9d1b89e8e6d8753" filehashsrc="test_list"
url="http://172.16.67.148/mhash_block.com" profile="mhash_test" agent="Firefox/43.0"
analyticssubmit="false"
```

External resources for DNS filter

External resources provides the ability to dynamically import an external block list into an HTTP server. This feature enables the FortiGate to retrieve a dynamic URL, domain name, IP address, or malware hash list from an external HTTP server periodically. The FortiGate uses these external resources as the web filter's remote categories, DNS filter's remote categories, policy address objects, or antivirus profile's malware definitions. If external resources are updated, FortiGate objects are also updated dynamically.

External resource is divided into four types:

- URL list (type = category)
- Domain name list (type = domain)
- IP address list (type = address)
- Malware hash list (type = malware)

Remote categories and external IP block list

The DNS filter profile can use two types of external resources: *domain type* (domain name list) and *address type* (IP address list).

When a *domain type* external resource is configured, it is treated as a remote category in the DNS filter profile. If the domain name in DNS query matches the entry in this external resource file, it is treated as the remote category and follows the action configured for this category in DNS filter profile.

When an *address type* external resource is configured, it can be enabled as *external-ip-blocklist* in DNS filter profile. If a DNS resolved IP address in DNS response matches the entry in the *external-ip-blocklist*, this DNS query is blocked by the DNS filter.

For external resources file format and limits, see [External resources file format on page 219](#).

Configuring external resources in the CLI

In the CLI, you can configure external resources files in an external HTTP server. Under global, configure the external resources file location and specify the resource type.

To configure external resources:

```
config system external-resource
    edit "Ext-Resource-Type-as-Domain-1"
```

```
        set type domain
        set category 194
        set resource "http://172.16.200.66/external-resources/Ext-Resource-Type-as-Domain-
1.txt"
        set refresh-rate 1
    next
    edit "Ext-Resource-Type-as-Address-1"
        set status enable
        set type address
        set username ''
        set password
        set comments ''
        set resource "http://172.16.200.66/external-resources/Ext-Resource-Type-as-Address-
1.txt"
        set refresh-rate 1
    next
end
```

In each VDOM, the domain type external resource can be used in the DNS filter as remote category. In this example, the domain name list in the Ext-Resource-Type-as-Domain-1.txt file is treated as a remote category (category ID 194). The IP address list in the Ext-Resource-Type-as-Address-1.txt file can be applied in the DNS filter as an external-ip-blocklist. If the DNS resolved IP address matches any entry in the list in that file, the DNS query is blocked.

To configure the external IP block list and apply it to a policy:

```
config dnsfilter profile
    edit "default"
        set comment "Default dns filtering."
        config ftgd-dns
            config filters
                edit 1
                    set category 194
                    set action block
                next
                edit 2
                    set category 12
                next
                edit 3
                next
            end
        end
        set block-botnet enable
        set external-ip-blocklist "Ext-Resource-Type-as-Address-1"
    next
end

config firewall policy
    edit 1
        set name "DNSFilter"
        set srcintf "port10"
        set dstintf "port9"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
```

```

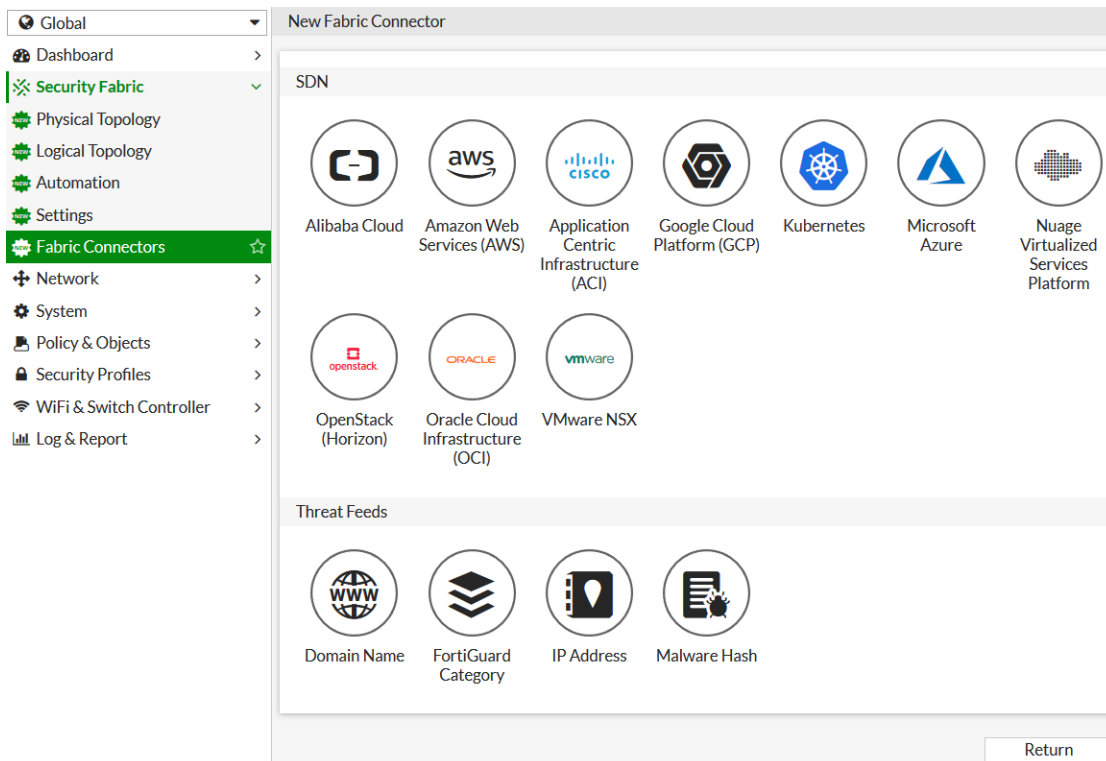
set utm-status enable
set logtraffic all
set dnsfilter-profile "default"
set profile-protocol-options "protocol"
set ssl-ssh-profile "protocols"
set nat enable
next
end

```

Configuring external resources in the GUI

To configure, edit, or view the entries for external resources from GUI:

1. Go to *Global > Security Fabric > Fabric Connectors*.
2. Click *Create New*.
3. In the *Threat Feeds* section, select *Domain Name* or *IP Address*.



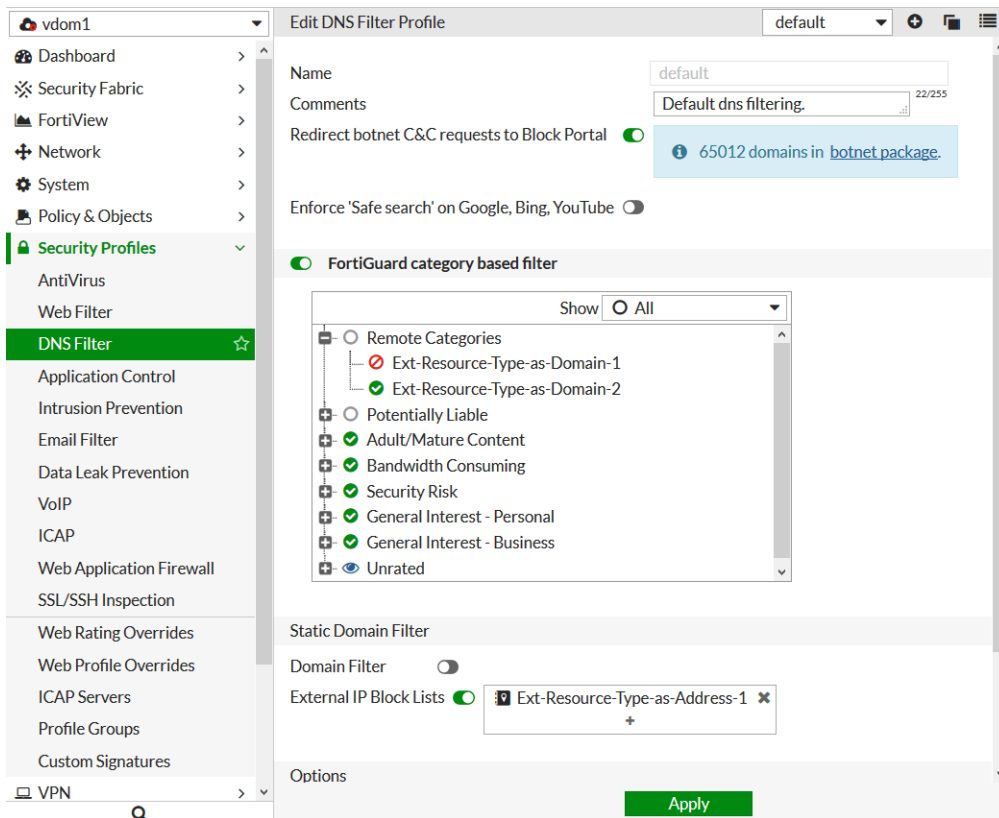
4. Enter the Resource *Name*, URL, location of the resource file, resource authentication credentials, and *Refresh Rate*.

5. Click OK.

6. Double-click the *Threat Feeds Object* you just configured to open the *Edit* page.7. Click *View Entries* to view the entry list in the external resources file.

Entry	Validity
www.example.com	Valid
www.fortinet.com	Valid

8. Go to *VDOM > Security Profiles > DNS Filter* and open a DNS filter profile. The configured external resources displays, and you can apply it in each DNS filter profile (remote category or external IP block lists).



Log sample

Remote categories

Go to **VDOM > Log & Report > DNS Query**. Some domains that match the remote category list are rated as remote category, overriding their original domain rating.

vdom1											
Log & Report											
DNS Type: dns - response Add Filter											
Date/Time	DNS Type	Source	Domain Name	Query Type	Policy	Message	Domain Filter List	Category	Category Description	Domain Filter Index	
2019/01/18 13:49:12	dns	10.1.100.18	www.example.com	A	1	Domain is monitored		196	Ext-Resource-Type-as-Domain-3		
2019/01/18 13:49:12	dns	10.1.100.18	www.example.com	A	1						

Log example:

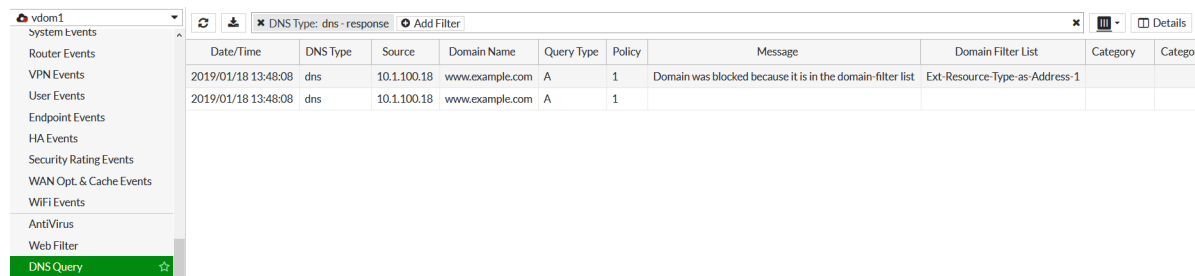
```
1: date=2019-01-18 time=13:49:12 logid="1501054802" type="utm" subtype="dns" eventtype="dns-response" level="notice" vd="vdom1" eventtime=1547848151 policyid=1 sessionid=82998 srcip=10.1.100.18 srcport=42985 srcintf="port10" srcintfrole="undefined" dstip=172.16.95.16
```

```
dstport=53 dstintf="port9" dstintfrole="undefined" proto=17 profile="default" xid=38234
qname="www.example.com" qtype="A" qtypeval=1 qclass="IN" ipaddr="93.184.216.34" msg="Domain
is monitored" action="pass" cat=196 catdesc="Ext-Resource-Type-as-Domain-3"
```

```
2: date=2019-01-18 time=13:49:12 logid="1500054000" type="utm" subtype="dns" eventtype="dns-
query" level="information" vd="vdom1" eventtime=1547848151 policyid=1 sessionid=82998
srcip=10.1.100.18 srcport=42985 srcintf="port10" srcintfrole="undefined" dstip=172.16.95.16
dstport=53 dstintf="port9" dstintfrole="undefined" proto=17 profile="default" xid=38234
qname="www.example.com" qtype="A" qtypeval=1 qclass="IN"
```

External IP block lists

Go to **VDOM > Log & Report > DNS Query**. If the DNS query resolved IP address matches the entry in the `external-ip-blocklist`, the DNS query is blocked.



Date/Time	DNS Type	Source	Domain Name	Query Type	Policy	Message	Domain Filter List	Category	Category Details
2019/01/18 13:48:08	dns	10.1.100.18	www.example.com	A	1	Domain was blocked because it is in the domain-filter list	Ext-Resource-Type-as-Address-1		
2019/01/18 13:48:08	dns	10.1.100.18	www.example.com	A	1				

Log example:

```
1: date=2019-01-18 time=13:50:53 logid="1501054400" type="utm" subtype="dns" eventtype="dns-
response" level="warning" vd="vdom1" eventtime=1547848253 policyid=1 sessionid=83206
srcip=10.1.100.18 srcport=47281 srcintf="port10" srcintfrole="undefined" dstip=172.16.95.16
dstport=53 dstintf="port9" dstintfrole="undefined" proto=17 profile="default" xid=7501
qname="www.example.com" qtype="A" qtypeval=1 qclass="IN" msg="Domain was blocked because it
is in the domain-filter list" action="redirect" domainfilteridx=0 domainfilterlist="Ext-
Resource-Type-as-Address-1"
```

```
2: date=2019-01-18 time=13:50:53 logid="1500054000" type="utm" subtype="dns" eventtype="dns-
query" level="information" vd="vdom1" eventtime=1547848253 policyid=1 sessionid=83206
srcip=10.1.100.18 srcport=47281 srcintf="port10" srcintfrole="undefined" dstip=172.16.95.16
dstport=53 dstintf="port9" dstintfrole="undefined" proto=17 profile="default" xid=7501
qname="www.example.com" qtype="A" qtypeval=1 qclass="IN"
```

Automation stitches

Automation stitches automate the activities between the different components in the Security Fabric, decreasing the response times to security events. Events from any source in the Security Fabric can be monitored, and action responses can be set up to any destination.



Automation stitches can also be used on FortiGate devices that are not part of a Security Fabric.

Automation stitches that use cloud-based actions, such as AWS Lambda and Azure Function, have the option to delay an action after the previous action is completed.

An automation stitch consists of two parts, the trigger and the actions. The trigger is the condition or event on the FortiGate that activates the action, for example, a specific log, or a failed log in attempt. The action is what the FortiGate does in response to the trigger.

Diagnose commands are available in the CLI to test, log, and display the history and settings of stitches.



Automation stitches can only be created on the root FortiGate in a Security Fabric.

Creating automation stitches

To create an automation stitch, a trigger event and a response action or actions are selected. Automation stitches can also be tested after they are created.

To create an automation stitch in the GUI:

1. On the root FortiGate, go to *Security Fabric > Automation*.
2. Click *Create New*. The *New Automation Stitch* page opens.

The screenshot shows the 'New Automation Stitch' configuration page. It includes a 'Name' text field, a 'Status' dropdown menu with 'Enabled' (green) and 'Disabled' (red) options, and a 'FortiGate' dropdown menu with 'All FortiGates' selected. Below these are two rows of circular icons representing triggers and actions. The 'Trigger' row includes: Compromised Host, Security Rating Summary, Configuration Change, Reboot, License Expiry, HA Failover, AV & IPS DB Update, FortiOS Event Log, FortiAnalyzer Event Handler, and Schedule. The 'Action' row includes: CLI Script, Email, FortiExplorer Notification, AWS Lambda, Azure Function, Google Cloud Function, AliCloud Function, and Webhook. At the bottom, there is a 'Minimum interval (seconds)' text field with the value '0'. The page concludes with 'OK' and 'Cancel' buttons.

New Automation Stitch

Name

Status Enabled Disabled

FortiGate All FortiGates

Trigger

Compromised Host Security Rating Summary Configuration Change Reboot License Expiry HA Failover AV & IPS DB Update FortiOS Event Log FortiAnalyzer Event Handler Schedule

Action

CLI Script Email FortiExplorer Notification AWS Lambda Azure Function Google Cloud Function AliCloud Function Webhook

Minimum interval (seconds)

OK Cancel

3. Enter the following information:

Name	Enter a name for the automation stitch.
Status	Enable/disable the stitch.
FortiGate	Select the FortiGate device to apply the automation stitch to, or select <i>All FortiGates</i> to apply it to all of them.
Trigger	Select a trigger.
Action	Select and configure one or more actions.
Minimum interval (seconds)	Enter a minimum time interval during which notifications for the same trigger event will not be sent. After the time interval elapses, an alert is sent that includes the last event since the time interval elapsed.

4. Click OK.

To create an automation stitch in the CLI:

1. Create an automation trigger:

```

config system automation-trigger
  edit <automation-trigger-name>
    set trigger-type {event-based | scheduled}
    set event-type <option>
    set license-type <option>
    set ioc-level {medium | high}
    set logid <integer>
    set trigger-frequency {hourly | daily | weekly | monthly}
    set trigger-weekday <option>
    set trigger-day <integer>
    set trigger-hour <integer>
    set trigger-minute <integer>
    set faz-event-severity <string>
    set faz-event-tags <string>
  next
end

```

The available options will vary depending on the selected event type.

2. Create an automation action:

```

config system automation-action
  edit <name>
    set action-type <option>
    set email-to <names>
    set email-from <string>
    set email-subject <string>
    set email-body <string>
    set minimum-interval <integer>
    set delay <integer>
    set required {enable | disable}
    set aws-api-id <string>
    set aws-region <string>
    set aws-domain <string>
  end
end

```

```

        set aws-api-stage <string>
        set aws-api-path <string>
        set aws-api-key <string>
        set azure-app <string>
        set azure-function <string>
        set azure-domain <string>
        set azure-function-authorization {anonymous | function | admin}
        set azure-api-key <string>
        set gcp-function-region <string>
        set gcp-project <string>
        set gcp-function-domain <string>
        set gcp-function <string>
        set alicloud-account-id <string>
        set alicloud-region <string>
        set alicloud-function-domain <string>
        set alicloud-version <string>
        set alicloud-service <string>
        set alicloud-function <string>
        set alicloud-function-authorization {anonymous | function}
        set alicloud-access-key-id <string>
        set alicloud-access-key-secret <string>
        set protocol {http | https}
        set method {post | put | get | patch | delete}
        set uri <string>
        set http-body <string>
        set port <integer>
        set headers <header>
        set script <string>
        set security-tag <string>
        set sdn-connector <connector_name>
    next
end

```

3. Create an automation destination:

```

config system automation-destination
    edit <name>
        set type {fortigate | ha-cluster}
        set destination <serial numbers>
        set ha-group-id <integer>
    next
end

```

4. Create the automation stitch:

```

config system automation-stitch
    edit <automation-stitch-name>
        set status {enable | disable}
        set trigger <trigger-name>
        set action <action-name>
        set destination <serial-number>
    next
end

```

To test an automation stitch:

In the GUI, go to *Security Fabric > Automation*, right-click on the automation stitch and select *Test Automation Stitch*.

In the CLI, enter the following command:

```
diagnose automation test <stitch-name> <log>
```

Chaining and delaying actions

Automation stitches that use cloud-based or webhook actions have the option to delay an action after the previous action is completed. The execution of the actions can be delayed by up to 3600 seconds (one hour).

To configure this option in the GUI, select a cloud-based action, then enter the required value, in seconds, in the action configuration's *Delay* field.

To configure a delay in the CLI, use the following command:

```
config system automation-action
  edit <name>
    set action-type {aws-lambda | azure-function | google-cloud-function | alicloud-
function | webhook}
    set required {enable | disable}
    set delay <seconds>
  next
end
```

Triggers

The following table outlines the available automation stitch triggers:

Trigger	Description
Compromised Host	<p>An Indicator of Compromise (IOC) is detected on a host endpoint.</p> <p>The threat level must be selected and can be <i>Medium</i> or <i>High</i>. If <i>Medium</i> is selected, both medium and high level threats are included.</p> <p>Note: Additional actions are available only for <i>Compromised Host</i> triggers:</p> <ul style="list-style-type: none"> • Access Layer Quarantine • Quarantine FortiClient via EMS • Assign VMware NSX Security Tag • IP Ban
Security Rating Summary	A summary is available for a recently run Security Rating.
Configuration Change	A FortiGate configuration change has occurred.
Reboot	A FortiGate is rebooting.
Low memory	<p>This option is only available in the CLI.</p> <p>Conserve mode due to low memory. See Execute a CLI script based on CPU and memory thresholds on page 264 for an example.</p>
High CPU	<p>This option is only available in the CLI.</p> <p>High CPU usage. See Execute a CLI script based on CPU and memory thresholds on page 264 for an example.</p>
License Expiry	<p>A FortiGuard license is expiring.</p> <p>The license type must be selected. Options include:</p>

Trigger	Description
	<ul style="list-style-type: none"> • FortiCare Support • FortiGuard Web Filter • FortiGuard AntiSpam • FortiGuard AntiVirus • FortiGuard IPS • FortiGuard Management Service • FortiGate Cloud
HA Failover	An HA failover is occurring.
AV & IPS DB Update	The antivirus and IPS database is updating.
FortiOS Event Log	<p>The specified FortiOS log has occurred.</p> <p>The event must be selected from the event list.</p>
FortiAnalyzer Event Handler	The specified FortiAnalyzer event handler has occurred. See FortiAnalyzer event handler trigger on page 238 for details.
Schedule	A scheduled monthly, weekly, daily, or hourly trigger. Set to occur on a specific minute of an specific hour on a specific day.
FortiGate Cloud-Based IOC	<p>IOC detection from the FortiGate Cloud IOC service.</p> <p>This option requires an IOC license, a web filter license, and FortiCloud logging must be enabled. See FortiGate Cloud-based IOC on page 303 for details.</p>

FortiAnalyzer event handler trigger

You can trigger automation stitches based on FortiAnalyzer event handlers. This allows you to define rules based on complex correlations across devices, log types, frequencies, and other criteria.

To set up a FortiAnalyzer event handler trigger:

1. [Configure a FortiGate event handler on the FortiAnalyzer](#)
2. [Configure FortiAnalyzer logging on the FortiGate on page 239](#)
3. [Configure an automation stitch that is triggered by a FortiAnalyzer event handler on page 240](#)

Configure a FortiGate event handler on the FortiAnalyzer

On the FortiAnalyzer, configure an event handler for the automation stitch. In this example, the event handler is triggered when an administrator logs in to the FortiGate.

To configure an event handler on the FortiAnalyzer:

1. Go to *Incidents & Events > Handlers > FortiGate Event Handlers*.
2. Configure an event handler for the automation stitch.

The screenshot shows the 'Create New Handler' configuration page in the FortiGate GUI. The page is titled 'Incidents & Events' and 'Create New Handler'. It includes fields for Name, Description, Devices, and Subnets. There are sections for Filters, Log Device Type, Log Type, Log Subtype, Group By, and Logs match. A table for Log Field, Match Criteria, and Value is shown. There is also a Generic Text Filter section and a Generate alert when section.

3. Click OK.

Configure FortiAnalyzer logging on the FortiGate

See [Configuring FortiAnalyzer on page 75](#) for more information.

To configure FortiAnalyzer logging in the GUI:

1. Go to *Security Fabric > Settings*.
2. Enable and configure *FortiAnalyzer Logging*.

The screenshot shows the 'Security Fabric Settings' page in the FortiGate GUI. The page is titled 'FortiGate 60E' and 'Security Fabric Settings'. It includes a section for 'FortiAnalyzer Logging' with fields for IP address, Logging to ADOM, Storage usage, Analytics usage, Archive usage, Upload option, SSL encrypt log transmission, and Allow access to FortiGate REST API. There is also a section for 'Cloud Solutions' with links to Amazon Web Services Marketplace, Introduction to FortiSandbox, and Configure FortiSandbox in AWS.

3. Click *Apply*.

To configure FortiAnalyzer logging in the CLI:

```
config log fortianalyzer setting
set status enable
set server "10.6.30.250"
set serial "FL-4HET318900407"
set upload-option realtime
```

```
set reliable enable
end
```

Configure an automation stitch that is triggered by a FortiAnalyzer event handler

When a FortiAnalyzer event handler is triggered, it sends a notification to the FortiGate automation framework, which generates a log and triggers the automation stitch.

To configure an automation stitch that is triggered by a FortiAnalyzer event handler in the GUI:

1. Go to *Security Fabric > Automation*.
2. Click *Create New*.
3. In the *Trigger* section, select *FortiAnalyzer Event Handler*.
4. Set *Event handler name* to the event that was created on the FortiAnalyzer.
5. Set the *Event severity*, and select or create an *Event tag*.

The screenshot shows the 'New Automation Stitch' configuration window in the FortiGate GUI. The left sidebar shows the navigation menu with 'Automation' selected. The main panel is divided into 'Trigger' and 'Action' sections. In the 'Trigger' section, 'FortiAnalyzer Event Handler' is selected. The 'Event handler name' is 'system-log-handler2', 'Event severity' is 'Medium', and 'Event tag' is 'User log in successful'. In the 'Action' section, 'Email' is selected. The email configuration fields are: 'To: brodriguez@fortinet.com', 'Email subject: FAZ Handler Event Trigger', and 'Email body: %%log%%'.

6. In the *Action* section, select *Email* and configure the email recipient and message.
7. Click *OK*.

To configure an automation stitch that is triggered by a FortiAnalyzer event handler in the CLI:

1. Create an automation action:

```
config system automation-action
  edit "auto-faz-1_email"
    set action-type email
    set email-to "jnjssll@fortinet.com"
    set email-subject "CSF stitch alert"
    set email-body "User login FortiGate successfully."
  next
end
```

2. Create an automation trigger:

```
config system automation-trigger
  edit "auto-faz-1"
```

```

set event-type faz-event
set faz-event-name "system-log-handler2"
set faz-event-severity "medium"
set faz-event-tags "User login successfully"
next
end

```

3. Create the automation stitch:

```

config system automation-stitch
edit "auto-faz-1"
set trigger "auto-faz-1"
set action "auto-faz-1_email"
next
end

```

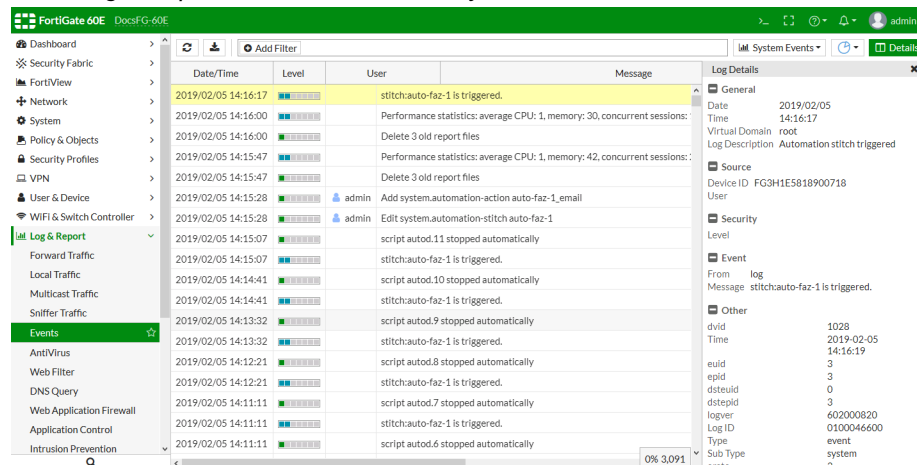
View the trigger event log

To see the trigger event log in the GUI:

1. Log in to the FortiGate.

The FortiAnalyzer sends notification to the FortiGate automation framework, generates an event log on the FortiGate, and triggers the automation stitch.

2. Go to *Log & Report > Events* and select *System Events*.



To see event logs in the CLI:

```
execute log display
```

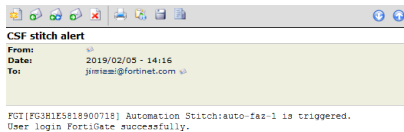
```

...
date=2019-02-05 time=14:16:17 logid="0100046600" type="event" subtype="system"
level="notice" vd="root" eventtime=1549404977 logdesc="Automation stitch triggered"
stitch="auto-faz-1" trigger="auto-faz-1" from="log" msg="stitch:auto-faz-1 is triggered."
...

```

Sample email

The email sent by the action will look similar to the following:



Actions

The following table outlines the available automation stitch actions. Multiple actions can be added and reorganized as needed by dragging and dropping.

Action	Description
Alert	Generate a FortiOS dashboard alert. This option is only available in the CLI.
CLI Script	Run one or more CLI scripts. See CLI script action on page 243 for details. See Execute a CLI script based on CPU and memory thresholds on page 264 for an example.
Disable SSID	Disable the SSID interface. This option is only available in the CLI.
Email	Send a custom email message to the selected recipients. At least one recipient and an email subject must be specified. The email body can use parameters from logs or previous action results. Wrapping the parameter with %% will replace the expression with the JSON value for the parameter, for example: <code>%%results.source%%</code> is the source property from the previous action.
FortiExplorer Notification	Send push notifications to FortiExplorer. The FortiGate must be registered to FortiCare on the iOS App that will receive the notification.
Access Layer Quarantine	This option is only available for Compromised Host triggers. Impose a dynamic quarantine on multiple endpoints based on the access layer.
Quarantine FortiClient via EMS	This option is only available for Compromised Host triggers. Use FortiClient EMS to block all traffic from the source addresses that are flagged as compromised hosts. Quarantined devices are flagged on the Security Fabric topology views. Go to <i>Monitor > Quarantine Monitor</i> to view and manage quarantined IP addresses.
Assign VMware NSX Security Tag	This option is only available for Compromised Host triggers. If an endpoint instance in a VMware NSX environment is compromised, the configured security tag is assigned to the compromised endpoint. See NSX Quarantine action on page 245 for details.
IP Ban	This option is only available for Compromised Host triggers. Block all traffic from the source addresses flagged by the IOC. Go to <i>Monitor > Quarantine Monitor</i> to view and manage banned IP addresses.

Action	Description
AWS Lambda	Send log data to an integrated AWS service. See AWS Lambda action on page 248 for details.
Azure Function	Send log data to an Azure function. See Azure Function action on page 250 for details.
Google Cloud Function	Send log data to a Google Cloud function. See Google Cloud Function action on page 252 for details.
AliCloud Function	Send log data to an AliCloud function. See AliCloud Function action on page 254 for details.
Webhook	Send an HTTP request using a REST callback. See Webhook action on page 257 for details, and Slack integration webhook on page 263 for an example.

CLI script action

CLI scripts can be run when an automation stitch is triggered. The scripts can be manually entered, uploaded as a file, or recorded in the CLI console. The output of the script can be sent as an email action.



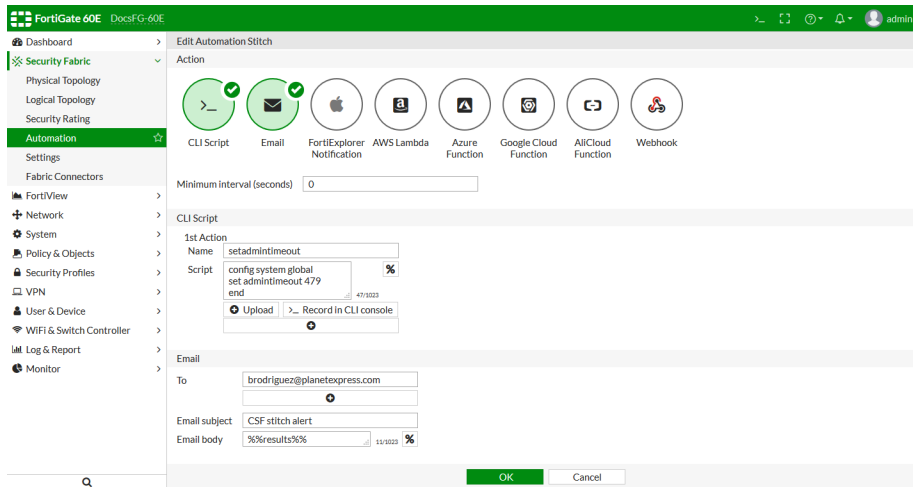
The maximum size of the CLI script action output is 4K characters.

In this example, the script sets the idle timeout value to 479 minutes, and sends an email with the script output.

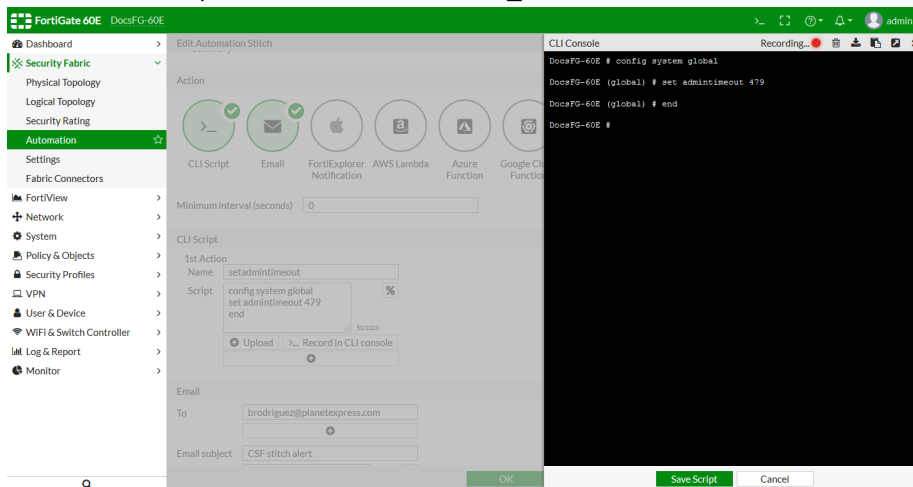
To configure a CLI script automation stitch in the GUI:

1. Go to *Security Fabric > Automation*.
2. Click *Create New*.
3. Enter a name for the stitch, and select the FortiGate devices that it will be applied to.
4. Select a trigger, such as *Security Rating Summary*.
5. Select *CLI Script* and *Email* actions.
6. Configure the CLI script:

- To manually enter the script, type it into the *Script* field.



- To upload a script file, click *Upload* and locate the file on your management computer.
- To record the script in the CLI console, click *>_Record in CLI console*, then enter the CLI commands.



- Configure the email action.
- Click *OK*.

To configure a CLI script automation stitch in the CLI:

- Create an automation action:

```
config system automation-action
  edit "set admintimeout479"
    set action-type cli-script
    set minimum-interval 0
    set delay 0
    set required enable
    set script "config system global
               set admin timeout 480
               end"
  next
  edit "auto-cli-1_email"
    set action-type email
```

```

        set email-to "jnkssl1@fortinet.com"
        set email-subject "CSF stitch alert"
        set email-body "%results%"
        set minimum-interval 0
    next
end

```

2. Create an automation trigger:

```

config system automation-trigger
    edit "auto-cli-1"
        set trigger-type event-based
        set event-type security-rating-summary
    next
end

```

3. Create the automation stitch:

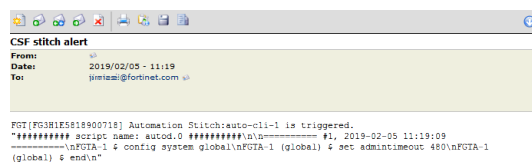
```

config system automation-stitch
    edit "auto-cli-1"
        set status enable
        set trigger "auto-cli-1"
        set action "set admintimeout479"
    next
end

```

Email sample

The email sent by the action will look similar to the following:



NSX Quarantine action

If an endpoint instance in a VMware NSX environment is compromised, this action will assign the configured security tag is to the compromised endpoint.

This action is only available when the automation trigger is set to compromised host.

To set up the NSX quarantine action, you need to:

1. [Configure a VMware NSX SDN connector](#)
2. [Configure an NSX security tag automation stitch](#)
3. [Configure FortiAnalyzer logging on the FortiGate](#)

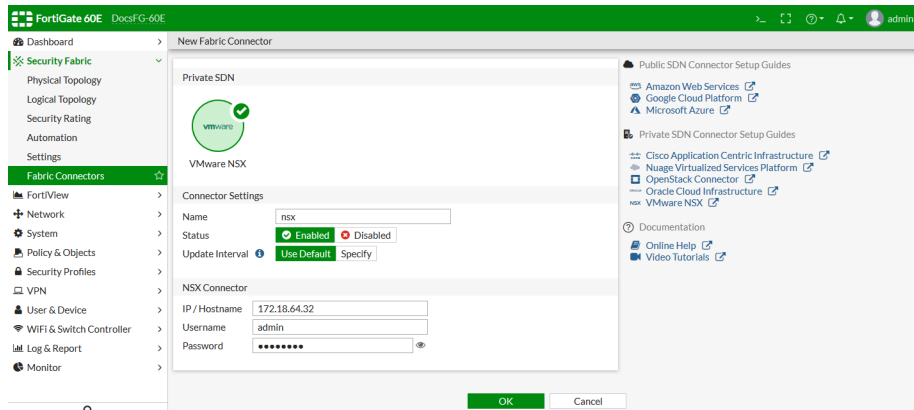
Configure a VMware NSX SDN connector

The FortiGate retrieves security tags from the VMware NSX server through the connector.

To configure a VMware NSX SDN connector in the GUI:

1. Go to *Security Fabric > Fabric Connectors*
2. Click *Create New*.

3. Select *VMware NSX*
4. Configure the settings.



5. Click **OK**.

To configure a VMware NSX SDN connector in the CLI:

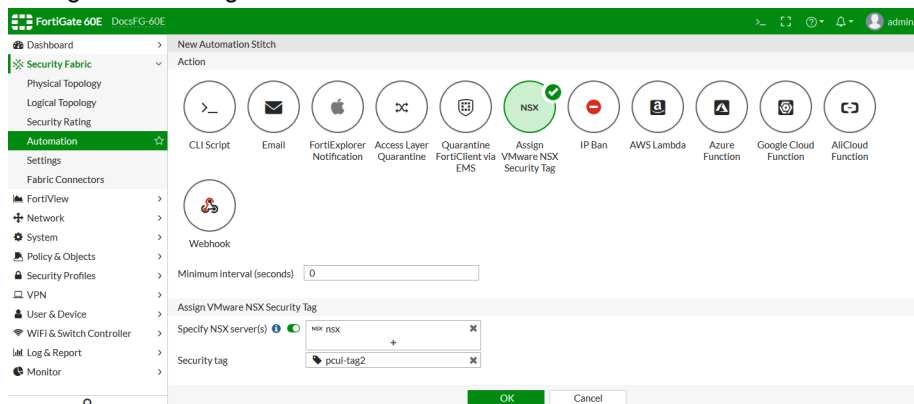
```
config system sdn-connector
  edit "nsx"
    set type nsx
    set server "172.18.64.32"
    set username "admin"
    set password xxxxxx
  next
end
```

Configure an NSX security tag automation stitch

Security tags are retrieved from the VMware NSX server through the NSX SDN connector.

To configure an NSX security tag automation stitch in the GUI:

1. Go to *Security Fabric > Automation*.
2. Click *Create New*.
3. In the *Trigger* section, select *Compromised Host*.
4. In the *Action* section, select *Assign VMware NSX Security Tag*.
5. Configure the settings.



- Click **OK**.

To configure an NSX security tag automation stitch in the CLI:

- Create an automation action:

```
config system automation-action
  edit "pcui-test_quarantine-nsx"
    set action-type quarantine-nsx
    set security-tag "pcui-tag2"
    set sdn-connector "nsx"
  next
end
```

- Create an automation trigger:

```
config system automation-trigger
  edit "pcui-test"
    set ioc-level high
  next
end
```

- Create the automation stitch:

```
config system automation-stitch
  edit "pcui-test"
    set trigger "pcui-test"
    set action "pcui-test_quarantine-nsx"
  next
end
```

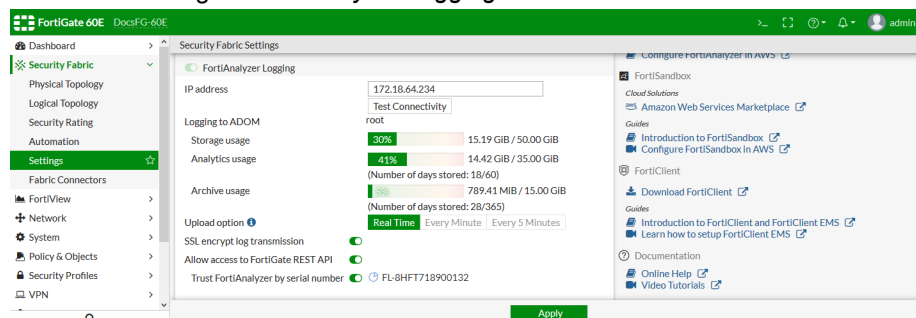
Configure FortiAnalyzer logging on the FortiGate

The FortiAnalyzer is used to send endpoint compromise notification to the FortiGate.

See [Configuring FortiAnalyzer on page 75](#) for more information.

To configure FortiAnalyzer logging in the GUI:

- Go to **Security Fabric > Settings**.
- Enable and configure **FortiAnalyzer Logging**.



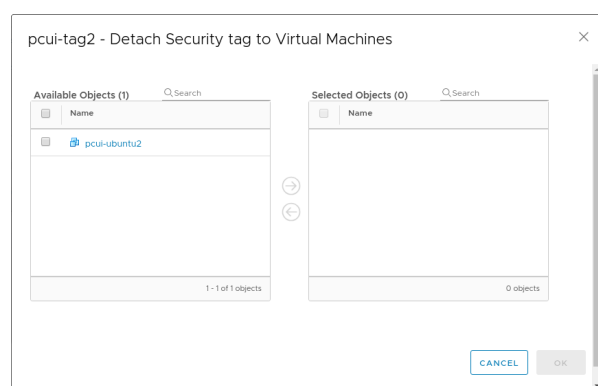
- Click **Apply**.

To configure FortiAnalyzer logging in the CLI:

```
config log fortianalyzer setting
  set status enable
  set server "172.18.64.234"
  set serial "FL-8HFT718900132"
  set upload-option realtime
  set reliable enable
end
```

When an endpoint instance is compromised

When an endpoint instance, such as *pcui-ubuntu2*, in the VMware NSX environment is compromised, the automation stitch is triggered. The FortiGate then assigns the configured security tag, *pcui-tag2* in this example, to the compromised NSX endpoint instance.

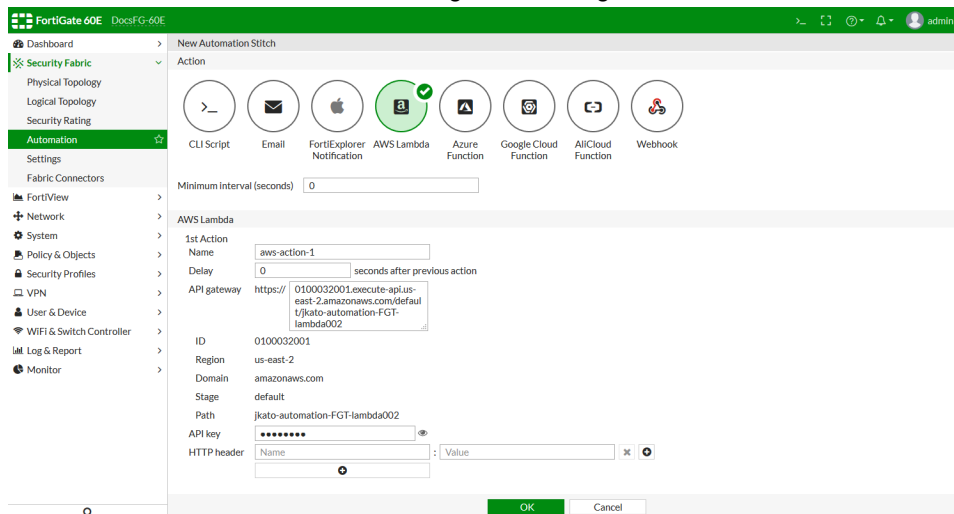
**AWS Lambda action**

AWS Lambda functions can be called when an automation stitch is triggered.

To configure an AWS Lambda function automation stitch in the GUI:

1. Go to *Security Fabric > Automation*.
2. Click *Create New*.
3. Enter a name for the stitch, and select the FortiGate devices that it will be applied to.
4. Select a trigger, such as *Security Rating Summary*.

5. Select *AWS Lambda Function* and configure its settings.



Name	The action name.
Delay	The amount of time after the previous action before this action executes, in seconds (0 - 3600, default = 0).
API gateway	The API gateway URL, in the format: <code>{restapi-id}.execute-api.{region}.{domain}/{stage}/{path}</code> The CLI must be used to manually enter the individual parameters.
API key	The API key configured in your API gateway.
HTTP header	The HTTP request header name and value. Multiple headers can be added.
+	Click to add another action. Actions can be reorganized as needed by dragging and dropping.
Name	The action name.
Delay	The amount of time after the previous action before this action executes, in seconds (0 - 3600, default = 0).

6. Click *OK*.

To configure an AWS Lambda function automation stitch in the CLI:

1. Create an automation action:

```
config system automation-action
  edit "aws-action-1"
    set action-type aws-lambda
    set aws-api-id "0100032001"
    set aws-region "us-east-2"
    set aws-api-stage "default"
    set aws-api-path "jkato-automation-FGT-lambda002"
    set aws-api-key ENC
nx8q830xafVTdmAKv77GIdLYthROoRXmtYsrpF4wtuvfIMlSHvHxE9EYo8W/jquj0p5GRsZOMDrgG1zB0oUq7bvo
guLUa/Jx4IV0DgwzOWRUruoWEIIHQBHJWSnnrswbw1O0Px+p3uz4azh4XkR+Vi+U8/ngGoLKLtwWHn53Oa4YbK7w
+mKz1BJVV+DlbCfDkPmPkA==
```

```

    next
end

```

2. Create an automation trigger:

```

config system automation-trigger
    edit "auto-aws"
        set event-type security-rating-summary
    next
end

```

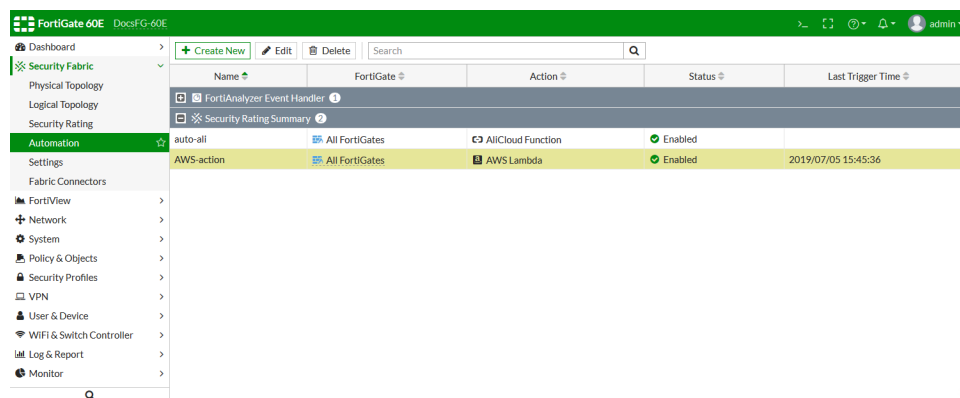
3. Create the automation stitch:

```

config system automation-stitch
    edit "auto-aws"
        set trigger "auto-aws"
        set action "aws-action-1"
    next
end

```

When the automation stitch is triggered, the FortiGate shows the stitch trigger time:



Name	FortiGate	Action	Status	Last Trigger Time
FortiAnalyzer Event Handler				
Security Rating Summary				
auto-all	All FortiGates	AllCloud Function	Enabled	
AWS-action	All FortiGates	AWS Lambda	Enabled	2019/07/05 15:45:36

In AWS, the log shows that the function was called, executed, and finished.

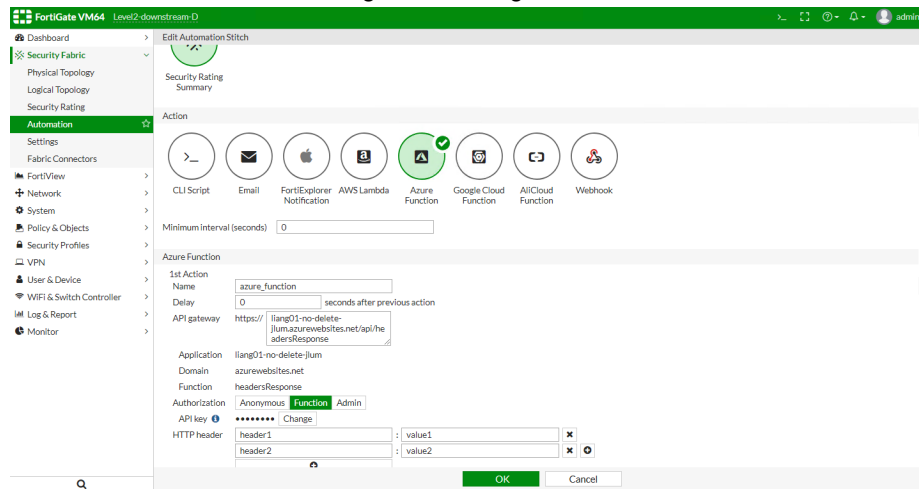
Azure Function action

Azure functions can be called when an automation stitch is triggered.

To configure an Azure function automation stitch in the GUI:

1. Go to *Security Fabric > Automation*.
2. Click *Create New*.
3. Enter a name for the stitch, and select the FortiGate devices that it will be applied to.
4. Select a trigger, such as *Security Rating Summary*.

5. Select *Azure Function* and configure its settings.



Name	The action name.
Delay	The amount of time after the previous action before this action executes, in seconds (0 - 3600, default = 0).
API gateway	The API gateway URL, in the format: <pre>{application}.{domain}/api/{function}</pre> The CLI must be used to manually enter the individual parameters.
Authorization	The authorization level: <i>Anonymous</i> , <i>Function</i> , or <i>Admin</i> .
API key	The API key configured in your API gateway. This options is only available when <i>Authorization</i> is not <i>Anonymous</i> .
HTTP header	The HTTP request header name and value. Multiple headers can be added.
+	Click to add another action. Actions can be reorganized as needed by dragging and dropping.

6. Click OK.

To configure an Azure function automation stitch in the CLI:

1. Create an automation action:

```
config system automation-action
  edit "azure_function"
    set action-type azure-function
    set azure-app "liang01-no-delete-jlum"
    set azure-function "headersResponse"
    set azure-function-authorization function
    set azure-api-key xxxxxx
    set headers "header1:value1" "header2:value2"
  next
end
```

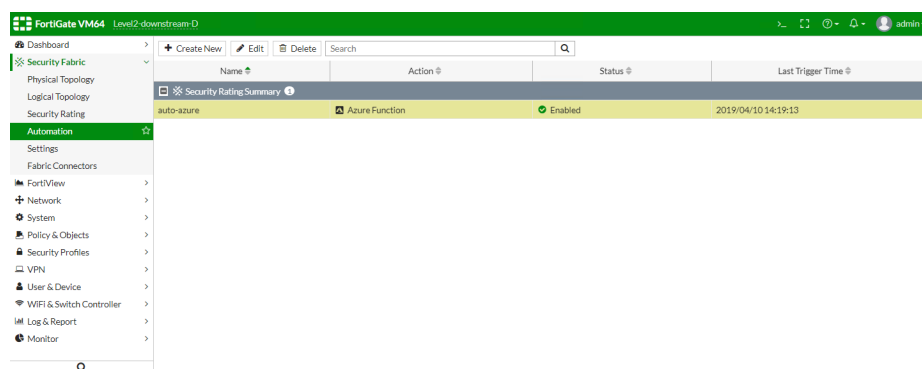
2. Create an automation trigger:

```
config system automation-trigger
  edit "auto-azure"
    set event-type security-rating-summary
  next
end
```

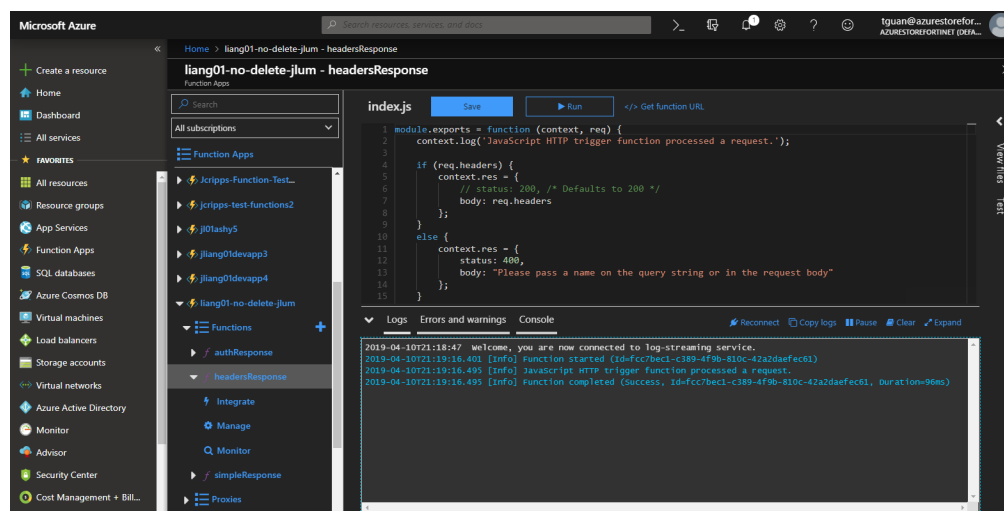
3. Create the automation stitch:

```
config system automation-stitch
  edit "auto-azure"
    set trigger "auto-azure"
    set action "azure_function"
  next
end
```

When the automation stitch is triggered, the FortiGate shows the stitch trigger time:



In Azure, the function log shows that the function was called, executed, and finished:

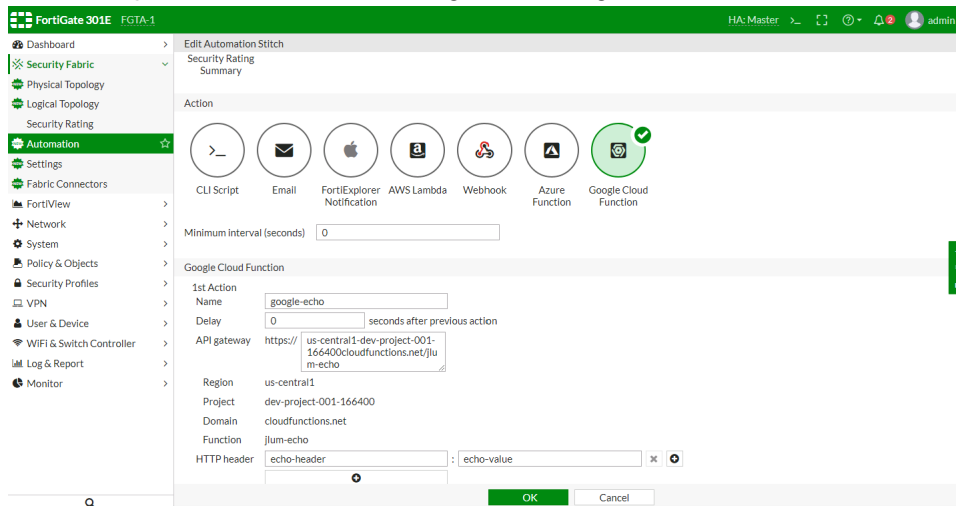


Google Cloud Function action

Google Cloud functions can be called when an automation stitch is triggered.

To configure a Google Cloud function automation stitch in the GUI:

1. Go to *Security Fabric > Automation*.
2. Click *Create New*.
3. Enter a name for the stitch, and select the FortiGate devices that it will be applied to.
4. Select a trigger, such as *Security Rating Summary*.
5. Select *Google Cloud Function* and configure its settings.



Name	The action name.
Delay	The amount of time after the previous action before this action executes, in seconds (0 - 3600, default = 0).
API gateway	<p>The API gateway URL, in the format:</p> <pre>{region}-{project}{domain}/{function}</pre> <p>The CLI must be used to manually enter the individual parameters.</p>
HTTP header	The HTTP request header name and value. Multiple headers can be added.
+	<p>Click to add another action.</p> <p>Actions can be reorganized as needed by dragging and dropping.</p>

6. Click *OK*.

To configure a Google Cloud function automation stitch in the CLI:

1. Create an automation action:

```
config system automation-action
    edit "google-echo"
        set action-type google-cloud-function
        set gcp-function-region "us-central1"
        set gcp-project "dev-project-001-166400"
        set gcp-function-domain "cloudfunctions.net"
        set gcp-function "jlum-echo"
        set headers "echo-header:echo-value"
    next
end
```

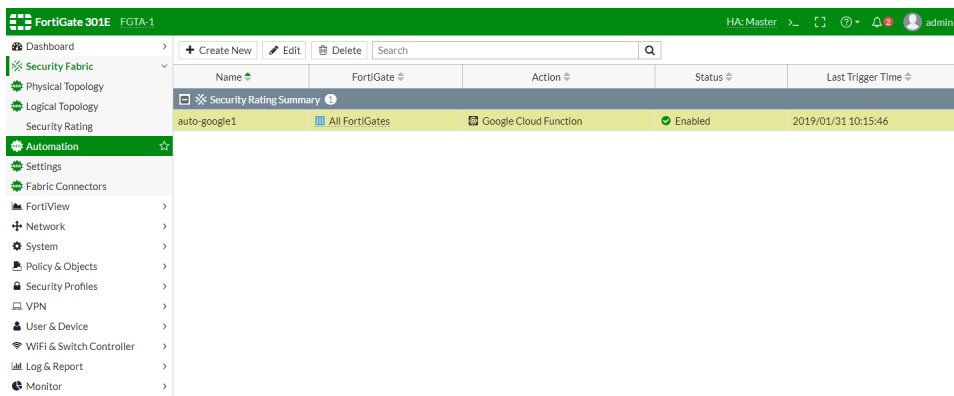
2. Create an automation trigger:

```
config system automation-trigger
  edit "auto-google1"
    set event-type security-rating-summary
  next
end
```

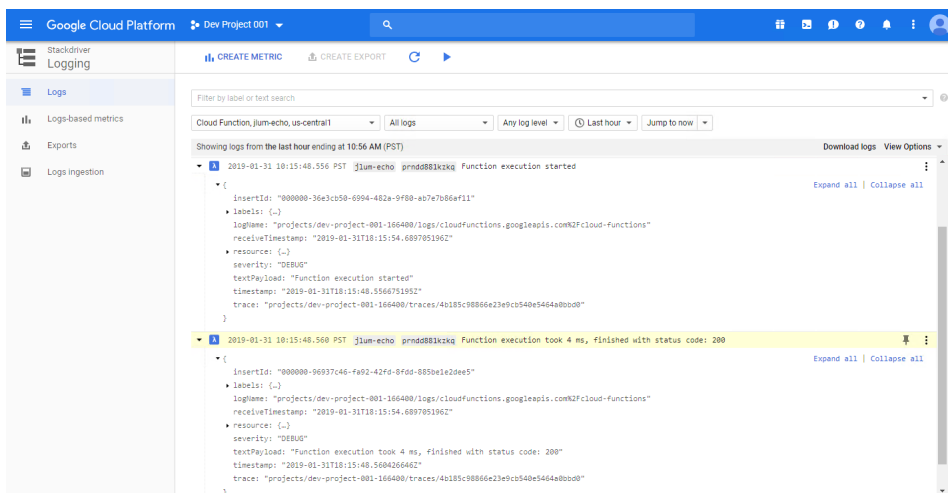
3. Create the automation stitch:

```
config system automation-stitch
  edit "auto-google1"
    set trigger "auto-google1"
    set action "google-echo"
  next
end
```

When the automation stitch is triggered, the FortiGate shows the stitch trigger time:



In Google Cloud, go to *Logs* to see the function log showing that the configured function was called, executed, and finished:



AliCloud Function action

AliCloud functions can be called when an automation stitch is triggered.

To configure an AliCloud function automation stitch in the GUI:

1. Go to *Security Fabric > Automation*.
2. Click *Create New*.
3. Enter a name for the stitch, and select the FortiGate devices that it will be applied to.
4. Select a trigger, such as *Security Rating Summary*.
5. Select *AliCloud Function* and configure its settings.

Name The action name.

Delay The amount of time after the previous action before this action executes, in seconds (0 - 3600, default = 0).

HTTP URL The HTTP URL, in the format:
`{account id}.{region}.{domain}/{version}/proxy/{service}/{function}`
 The CLI must be used to manually enter the individual parameters.

Authorization The authorization level: *Anonymous*, or *Function*.

AccessKey ID The access key ID
 This options is only available when *Authorization* is *Function*.

AccessKey Secret The access key secret.
 This options is only available when *Authorization* is *Function*.

HTTP header The HTTP request header name and value. Multiple headers can be added.

+ Click to add another action.
 Actions can be reorganized as needed by dragging and dropping.

6. Click *OK*.

To configure an AliCloud function automation stitch in the CLI:

1. Create an automation action:

```
config system automation-action
  edit "Ali-Action-1"
    set action-type alicloud-function
    set alicloud-account-id "5594200612296301"
    set alicloud-region "us-east-1"
    set alicloud-version "2016-08-15"
    set alicloud-service "jlum-test-function"
    set alicloud-function "echoBodyAuth"
    set alicloud-function-authorization function
    set alicloud-access-key-id "LTAIKmERWEuEOChg"
    set alicloud-access-key-secret xxxxxx
  next
end
```

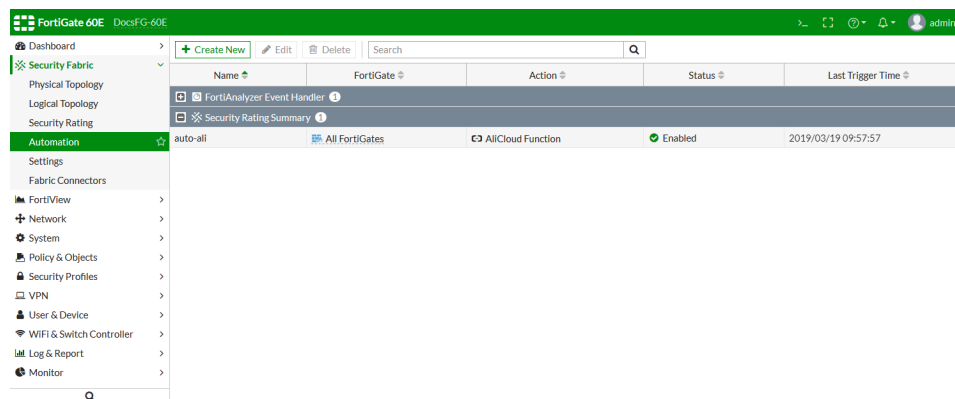
2. Create an automation trigger:

```
config system automation-trigger
  edit "auto-ali"
    set event-type security-rating-summary
  next
end
```

3. Create the automation stitch:

```
config system automation-stitch
  edit "auto-ali"
    set trigger "auto-ali"
    set action "Ali-Action-1"
  next
end
```

When the automation stitch is triggered, the FortiGate shows the stitch trigger time:



Name	FortiGate	Action	Status	Last Trigger Time
FortiAnalyzer Event Handler				
Security Rating Summary				
auto-ali	All FortiGates	AliCloud Function	Enabled	2019/03/19 09:57:57

In AliCloud, the function log shows that the function was called, executed, and finished:

The screenshot shows the Fortinet Security Fabric console interface. On the left is a sidebar with navigation options like 'Overview', 'Functions', and 'Log'. The main area displays the 'Log' tab for the 'echoBodyAuth' function. It shows a list of log entries with columns for index, timestamp, and message. The messages are JSON objects containing details about security events, such as login attempts and ratings.

Webhook action

The webhook automation stitch action makes HTTP and HTTPS requests to a specified server, with custom headers, bodies, ports, and methods. It can be used to leverage the ubiquity of HTML requests and APIs to integrate with many other tools.



The URI and HTTP body can use parameters from logs or previous action results. Wrapping the parameter with `%%` will replace the expression with the JSON value for the parameter, for example: `%%results.source%%` is the source property from the previous action.

In this example, a specific log message (failed administrator log in attempt) triggers the FortiGate to send the contents of the log to a server. The server responds with a generic reply. This example assumes that the server is already configured and able to communicate with the FortiGate.

To configure the webhook automation stitch in the GUI:

1. Go to *Security Fabric > Automation*.
2. Click *Create New*.
3. Enter a name for the stitch, and select the FortiGate devices that it will be applied to.
4. Select the trigger *FortiOS Event Log*.
5. Set *Event* to *Admin login failed*.

6. Select *Webhook* and configure the settings:

The screenshot shows the FortiGate 60E GUI with the 'New Automation Stitch' configuration page. The left sidebar shows the 'Automation' menu. The main area is divided into 'Trigger' and 'Action' sections. The 'Trigger' is set to 'FortiOS Event Log' with the event 'Admin login failed'. The 'Action' is 'Webhook'. The 'Webhook' settings are as follows:

- 1st Action Name: Send Log To Server
- Delay: 0 seconds after previous action
- Protocol: HTTP
- Method: POST
- URI: http://172.16.200.44
- Port: 80
- HTTP body: %log%
- HTTP header: Header : 1st Action

Name	The action name.
Delay	The amount of time after the previous action before this action executes, in seconds (0 - 3600, default = 0).
Protocol	The request protocol to use: <i>HTTP</i> or <i>HTTPS</i> .
Method	The request method: <i>POST</i> , <i>PUT</i> , <i>GET</i> , <i>PATCH</i> , or <i>DELETE</i> .
URI	The request API URI.
Port	The protocol port.
HTTP body	The request body, if required, as a serialized JSON string. Use the parameter <i>%%log%%</i> to send the contents of the log from the trigger.
HTTP header	The HTTP request header name and value.
+	Click to add another action. Actions can be reorganized as needed by dragging and dropping.

7. Click *OK*.

To configure the webhook automation stitch in the CLI:

1. Create the automation action:

```
config system automation-action
edit "Send Log To Server"
set action-type webhook
set uri "172.16.200.44"
```



```

        set http-body "%log%"
        set port 80
        set headers "Header:1st Action"
    next
end

```

2. Create an automation trigger:

```

config system automation-trigger
    edit "badLogin"
        set event-type event-log
        set logid 32002
    next
end

```

3. Create the automation stitch:

```

config system automation-stitch
    edit "badLogin"
        set trigger "badLogin"
        set action "Send Log To Server"
    next
end

```

To test the automation stitch:

1. Attempt to log in to the FortiGate with an incorrect username or password.
2. On the server, check the log to see that its contents have been sent by the FortiGate.

```

..bf781718-A--
[30/May/2019:16:44:45 -0700] XPBq7mQycwAAENpZNoAAAD 172.16.200.5 19028 172.16.200.44 80
..bf781718-S--
POST / HTTP/1.1
Host: 172.16.200.44
Accept: */*
Header: 1st Action
Content-Length: 408
Content-Type: application/x-www-form-urlencoded
..bf781718-C--
date=2019-05-30 time=16:44:43 logid="0100032002" type="event" subtype="system" level="alert" vd="root" eventtime=1559250884209355090 tx="0700" logdesc="Admin login failed" src="0" user="admin" url="http(10.6.30.254)" method="http" srcip=10.6.30.254 dstip=10.6.30.3 action="login" status="failed" reason="passwd_invalid" msg="Administrator admin login failed from http(10.6.30.254) Because of invalid password"
..bf781718-F--
HTTP/1.1 200 OK
Upgrade: h2,h2c
Connection: Upgrade
Last-Modified: Thu, 30 May 2019 21:46:33 GMT
ETag: "01-35a21d4dcffa"
Accept-Ranges: bytes
Content-Length: 97
Vary: Accept-Encoding
Content-Type: text/html
..bf781718-E--
{
  "userId": 1,
  "id": 1,
  "title": "Test Response",
  "body": "ABCDEFGHIJKLMNQRSTUWXYZ"
}

```

The body content is replaced with the log of the trigger.

3. On the FortiGate, go to **Log & Report > Events** and select **System Events** to confirm that the stitch was activated.

Date/Time	Level	User	Message
2019/07/10 11:36:02	Alert	admin	stitch:badLogin is triggered.
2019/07/10 11:36:02	Alert	admin	Administrator admin login failed from https(172.27.2.206)
2019/07/10 11:35:30	Info	Fortimanager_Access	System config file has been downloaded by user Fortimanager
2019/07/10 11:35:24	Info	admin	Add system.automation-trigger badLogin
2019/07/10 11:35:24	Info	admin	Add system.automation-action Send Log To Server
2019/07/10 11:35:24	Info	admin	Add system.automation-stitch badLogin
2019/07/10 11:34:57	Info		Performance statistics: average CPU: 0, memory: 50, concu
2019/07/10 11:32:04	Info		FortiCloud 173.243.132.165 server is connected
2019/07/10 11:29:56	Info		Performance statistics: average CPU: 0, memory: 50, concu
2019/07/10 11:29:06	Info		FortiSandbox AV database updated
2019/07/10 11:24:57	Info		Performance statistics: average CPU: 0, memory: 50, concu
2019/07/10 11:19:57	Info		Performance statistics: average CPU: 0, memory: 51, concu
2019/07/10 11:19:35	Info	admin	Administrator admin logged in successfully from https(172.
2019/07/10 11:19:07	Info		FortiSandbox AV database updated
2019/07/10 11:14:57	Info		Performance statistics: average CPU: 0, memory: 50, concu
2019/07/10 11:09:57	Info		Performance statistics: average CPU: 2, memory: 50, concu
2019/07/10 11:04:56	Info		Performance statistics: average CPU: 0, memory: 50, concu
2019/07/10 10:59:58	Info		DHCP statistics
2019/07/10 10:59:56	Info		Performance statistics: average CPU: 0, memory: 50, concu
2019/07/10 10:57:05	Info		FortiSandbox AV database updated
2019/07/10 10:54:57	Info		Performance statistics: average CPU: 5, memory: 50, concu
2019/07/10 10:49:57	Info		Performance statistics: average CPU: 6, memory: 50, concu
2019/07/10 10:45:06	Info		FortiSandbox AV database updated
2019/07/10 10:44:57	Info		Performance statistics: average CPU: 4, memory: 50, concu

4. Go to **Security Fabric > Automation** to see the last time that the stitch was triggered.

Name	FortiGate	Action	Status	Last Trigger Time
FortiAnalyzer Event Handler				
FortiOS Event Log				
badLogin	All FortiGates	Webhook	Enabled	2019/07/10 11:36:51
Security Rating Summary				

Diagnose commands

- Enable log dumping:

```
# diagnose test application autod 1
```

```
autod dumped total:1 logs, num of logids:1
```

```
autod log dumping is enabled
```

```
vdom:root(0) logid:32002 len:408 log:
```

```
date=2019-05-30 time=17:41:03 logid="0100032002" type="event" subtype="system"
level="alert" vd="root" eventtime=1559263263858888451 tz="-0700" logdesc="Admin login
failed" sn="0" user="admin" ui="http(10.6.30.254)" method="http" srcip=10.6.30.254
dstip=10.6.30.5 action="login" status="failed" reason="passwd_invalid"
msg="Administrator admin login failed from http(10.6.30.254) because of invalid
password"
```

```
autod log dumping is disabled
```

```
autod logs dumping summary:
```

```
logid:32002 count:1
```

```
autod dumped total:1 logs, num of logids:1
```

- Show automation settings:

```
# diagnose test application autod 2
csf: enabled  root:yes
total stitches activated: 2

stitch: badLogin
  destinations: all
  trigger: badLogin

  local hit: 6 relayed to: 6 relayed from: 6
  actions:
    Send Log To Server type:webhook interval:0
      delay:0 required:no
      proto:0 method:0 port:80
      uri: 172.16.200.44
      http body: %%log%%
      headers:
        0. Header:1st Action
```

- Show automation statistics:

```
# diagnose test application autod 3

stitch: badLogin

  local hit: 1 relayed to: 1 relayed from: 1
  last trigger:Wed Jul 10 12:14:14 2019
  last relay:Wed Jul 10 12:14:14 2019

  actions:
    Send Log To Server:
      done: 1 relayed to: 1 relayed from: 1
      last trigger:Wed Jul 10 12:14:14 2019
      last relay:Wed Jul 10 12:14:14 2019

logid2stitch mapping:
id:32002  local hit: 3 relayed to: 3 relayed from: 3
  badLogin

action run cfg&stats:
total:55 cur:0 done:55 drop:0
  email:
    flags:10
    stats: total:4 cur:0 done:4 drop:0
  ios-notification:
    flags:1
    stats: total:0 cur:0 done:0 drop:0
  alert:
    flags:0
    stats: total:0 cur:0 done:0 drop:0
  disable-ssid:
    flags:7
    stats: total:0 cur:0 done:0 drop:0
  quarantine:
    flags:7
    stats: total:0 cur:0 done:0 drop:0
```

```

quarantine-forticlient:
    flags:4
    stats: total:0 cur:0 done:0 drop:0
quarantine-nsx:
    flags:4
    stats: total:0 cur:0 done:0 drop:0
ban-ip:
    flags:7
    stats: total:0 cur:0 done:0 drop:0
aws-lambda:
    flags:11
    stats: total:21 cur:0 done:21 drop:0
webhook:
    flags:11
    stats: total:6 cur:0 done:6 drop:0
cli-script:
    flags:10
    stats: total:4 cur:0 done:4 drop:0
azure-function:
    flags:11
    stats: total:0 cur:0 done:0 drop:0
google-cloud-function:
    flags:11
    stats: total:0 cur:0 done:0 drop:0
alicloud-function:
    flags:11
    stats: total:20 cur:0 done:20 drop:0

```

- Enable debug output and turn on automation debug messages for about 30 minutes:

```

# diagnose debug enable
# diagnose debug application autod -1

__auto_generate_generic_curl_request()-358: Generating generic automation CURL request
for action (Send Log To Server).
__auto_generate_generic_curl_request()-406: Generic automation CURL request POST data
for action (Send Log To Server):
date=2019-05-30 time=16:44:43 logid="0100032002" type="event" subtype="system"
level="alert" vd="root" eventtime=1559259884209355090 tz="-0700" logdesc="Admin login
failed" sn="0" user="admin" ui="http(10.6.30.254)" method="http" srcip=10.6.30.254
dstip=10.6.30.5 action="login" status="failed" reason="passwd_invalid"
msg="Administrator admin login failed from http(10.6.30.254) because of invalid
password"

__auto_generic_curl_request_close()-512: Generic CURL request response body from
http://172.16.200.44:
{
    "userId": 1,
    "id": 1,
    "title": "Test Response",
    "body": "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
}

```

Slack integration webhook

A webhook can be created to post messages and notifications to Slack. For information about using incoming webhooks in Slack, see <https://api.slack.com/incoming-webhooks>.

In this example, a configuration change triggers the FortiGate to post a message to Slack.

To create a webhook automation stitch for Slack integration in the GUI:

1. Go to *Security Fabric > Automation*.
2. Click *Create New*.
3. Enter a name for the stitch.
4. Select the trigger *Configuration Change*.
5. Select *Webhook* and configure the settings:

The screenshot shows the FortiGate 60E GUI with the 'Automation' section selected in the left sidebar. The 'Edit Automation Stitch' window is open, showing the following configuration:

- Name:** Slack
- Status:** Enabled
- Trigger:** Configuration Change
- Action:** Webhook (selected from a list of actions including CLI Script, Email, FortiExplorer Notification, AWS Lambda, Azure Function, Google Cloud Function, and AIICloud Function)
- Minimum interval (seconds):** 0
- Webhook configuration:**
 - 1st Action Name:** send to Slack
 - Delay:** 0 seconds after previous action
 - Protocol:** HTTP
 - Method:** POST
 - URI:** https://hooks.slack.com/services/XXXXXXXXXX/XXXXXXXXXX/XXXXXXXXXX
 - Port:** 443
 - HTTP body:** {"channel": "#delivery", "username": "tleela", "text": "Configuration changed", "icon_emoji": ":worried:"}
 - HTTP header:** Content-type: application/json

6. Click **OK**.

To create a webhook automation stitch for Slack integration in the CLI:

1. Create the automation action:

```
config system automation-action
  edit "send to Slack"
    set action-type webhook
    set protocol https
    set uri "hooks.slack.com/services/XXXXXXXXXX"
    set http-body '{"channel": "\#delivery", "username": "\tleela", "text":
  "\Configuration changed", "icon_emoji": "\:worried:"}'
    set port 443
    set headers "Content-type:application/json"
  next
end
```

2. Create the automation trigger:

```
config system automation-trigger
  edit "config change"
    set event-type config-change
  next
end
```

3. Create the automation stitch:

```
config system automation-stitch
  edit "Slack"
    set trigger "config change"
    set action "send to Slack"
  next
end
```

Execute a CLI script based on CPU and memory thresholds

Automation stitches can be created to run a CLI script and send an email message when CPU or memory usage exceeds specified thresholds.

In this example, two automation stitches are created that run a CLI script to collect debug information, and then email the results of the script to a specified email address when CPU usage threshold is exceeded or memory usage causes the FortiGate to enter conserve mode.



Automation stitches that use *High CPU* and *Conserve Mode* triggers can only be created in the CLI. Once create, they can be edited in the GUI.

To define CPU and memory usage thresholds:

```
config system global
  set cpu-use-threshold <percent>
  set memory-use-threshold-extreme <percent>
  set memory-use-threshold-green <percent>
  set memory-use-threshold-red <percent>
end
```

Where:

cpu-use-threshold	Threshold at which CPU usage is reported, in percent of total possible CPU utilization (default = 90).
memory-use-threshold-extreme	Threshold at which memory usage is considered extreme, and new sessions are dropped, in percent of total RAM (default = 95).
memory-use-threshold-green	Threshold at which memory usage forces the FortiGate to exit conserve mode, in percent of total RAM (default = 82).
memory-use-threshold-red	Threshold at which memory usage forces the FortiGate to enter conserve mode, in percent of total RAM (default = 88).

Configure the automation stitches

High CPU usage stitch

To create an automation stitch for high CPU usage:

1. Create an automation action to run a CLI script:

```
config system automation-action
    edit "high_cpu_debug"
        set action-type cli-script
        set required enable
        set script "diagnose debug cli 8
diagnose debug console timestamp enable
diagnose debug enable
diagnose debug crashlog read
get system performance status
get system session status
diagnose sys session full-stat
diagnose firewall iprope state
diagnose sys flash list
diagnose hardware sysinfo memory
diagnose hardware sysinfo slab
diagnose hardware sysinfo shm
diagnose hardware deviceinfo disk
get system arp
diagnose ip arp list
diagnose ip address list
get router info routing-table all
get router info kernel
diagnose ip rtcache list
diagnose sys top-summary
diagnose sys top 9 99"
    next
end
```

2. Create an automation action to send an email:

```
config system automation-action
    edit "auto_high_cpu_email"
        set action-type email
        set email-to "person@fortinet.com"
        set email-subject "CSF stitch alert: high_cpu"
        set email-body "%results%"
    next
end
```

3. Create an automation trigger:

```
config system automation-trigger
    edit "auto_high_cpu"
        set event-type high-cpu
    next
end
```

4. Create an automation stitch:

```
config system automation-stitch
    edit "auto_high_cpu"
        set trigger "auto_high_cpu"
        set action "high_cpu_debug" "auto_high_cpu_email"
    next
end
```

To edit the automation stitch in the GUI:

1. Go to *Security Fabric > Automation*.
2. Double click on the *auto_high_cpu* stitch.

The screenshot shows the FortiGate 60E GUI with the 'Edit Automation Stitch' window open. The left sidebar shows the navigation menu with 'Automation' selected. The main panel displays the configuration for the 'auto_high_cpu' stitch. The 'Name' field is 'auto_high_cpu' and the 'Status' is 'Enabled'. The 'Trigger' is 'High CPU'. The 'Action' section shows a list of available actions: CLI Script, Email, FortiExplorer Notification, AWS Lambda, Azure Function, Google Cloud Function, AllCloud Function, and Webhook. The 'Minimum Interval (seconds)' is set to 0. The 'CLI Script' section shows the '1st Action' with the name 'high_cpu_debug' and a script that runs various diagnostic commands. The 'Email' section shows the 'To' field as 'person@fortinet.com', the 'Email subject' as 'CSF stitch alert: high_cpu', and the 'Email body' as '%results%'.

3. Edit the stitch as required, then click **OK**.

High memory usage stitch

To create an automation stitch for high memory usage:

1. Create an automation action to run a CLI script:

```
config system automation-action
    edit "high_memory_debug"
        set action-type cli-script
        set required enable
        set script "diagnose debug cli 8
diagnose debug console timestamp enable
diagnose debug enable
```



```
diagnose debug crashlog read
get system performance status
get system session status
diagnose sys session full-stat
diagnose firewall iprope state
diagnose sys flash list
diagnose hardware sysinfo memory
diagnose hardware sysinfo slab
diagnose hardware sysinfo shm
diagnose hardware deviceinfo disk
get system arp
diagnose ip arp list
diagnose ip address list
get router info routing-table all
get router info kernel
diagnose ip rtcache list
diagnose sys top-summary
diagnose sys top 9 99"
    next
end
```

2. Create an automation action to send an email:

```
config system automation-action
    edit "auto_high_memory_email"
        set action-type email
        set email-to "person@fortinet.com"
        set email-subject "CSF stitch alert: high_memory"
        set email-body "%results%"
    next
end
```

3. Create an automation trigger:

```
config system automation-trigger
    edit "auto_high_memory"
        set event-type low-memory
    next
end
```

4. Create an automation stitch:

```
config system automation-stitch
    edit "auto_high_memory"
        set trigger "auto_high_memory"
        set action "high_memory_debug" "auto_high_memory_email"
    next
end
```

To edit the automation stitch in the GUI:

1. Go to *Security Fabric > Automation*.
2. Double click on the *auto_high_memory* stitch.

The screenshot shows the 'Edit Automation Stitch' window in the FortiGate 60E GUI. The left sidebar shows the navigation menu with 'Automation' selected. The main panel displays the configuration for the 'auto_high_memory' stitch. The 'Name' field is 'auto_high_memory' and the 'Status' is 'Enabled'. The 'Trigger' is 'Conserve Mode'. The 'Action' section shows a list of available actions: CLI Script, Email, FortiExplorer Notification, AWS Lambda, Azure Function, Google Cloud Function, AliCloud Function, and Webhook. The 'Minimum Interval (seconds)' is set to 0. The 'CLI Script' section shows the '1st Action' with the name 'high_memory_debug' and a script containing various diagnostic commands. The 'Email' section shows the 'To' field as 'person@fortinet.com', the 'Email subject' as 'CSF stitch alert: high_memory', and the 'Email body' as '%results%'. The 'OK' and 'Cancel' buttons are at the bottom.

3. Edit the stitch as required, then click **OK**.

Results

When FortiGate enters conserve mode due to the `memory-use-threshold-red` being exceeded, the GUI displays a notice, and the *auto_high_memory* automation stitch is triggered, causing the CLI script to run and the results of the script to be emailed to the specified address.

The screenshot shows the 'Automation' section in the FortiGate 60E GUI. A red banner at the top indicates 'Conserve mode activated due to high memory usage'. Below the banner is a table of automation stitches. The table has columns for Name, Action, Status, and Last Trigger Time. The stitches listed are 'Conserve Mode', 'auto_high_memory', 'High CPU', and 'auto_high_cpu'.

Name	Action	Status	Last Trigger Time
Conserve Mode			
auto_high_memory	>_ CLI Script ✉ Email	Enabled	2019/11/21 10:45:33
High CPU			
auto_high_cpu	>_ CLI Script ✉ Email	Enabled	2019/11/21 10:45:37

Here is an example of the email message:

```
CSF stitch alert: high_memory
noreply@notification.fortinet.net
Thu 11/21/2019 11:06 AM
James Li
FGT[FGVM16TM19000026] Automation Stitch:auto_high_memory is triggered.
##### script name: autod.47 #####
===== #1, 2019-11-21 11:07:24 =====
FGVM16TM19000026 $ diag deb cli 8
Debug messages will be on for 25 minutes.
FGVM16TM19000026 $ diag deb console timestamp enable
FGVM16TM19000026 $ diag deb enable
FGVM16TM19000026 $ diag deb crashlog read
1: 2019-08-08 11:35:25 the killed daemon is /bin/dhcpd: status=0x0
2: 2019-08-08 17:52:47 the killed daemon is /bin/pyfcgid: status=0x0
3: 2019-08-23 11:32:31 from=license status=INVALID
4: 2019-08-23 11:32:32 from=license status=INVALID
5: 2019-11-21 09:53:31 from=license status=VALID
...
```

Troubleshooting

The following topics provide troubleshooting information for the Fortinet Security Fabric:

- [Viewing a summary of all connected FortiGates in a Security Fabric on page 269](#)
- [Diagnosing automation stitches on page 272](#)

Viewing a summary of all connected FortiGates in a Security Fabric

In downstream FortiGates, the `diagnose sys csf global` command shows a summary of all of the connected FortiGates in the Security Fabric.

To view a Security Fabric summary on a downstream FortiGate:

```
# diagnose sys csf global
Current vision:
[
  {
    "path": "FGVM01TM19000001",
    "mgmt_ip_str": "104.196.102.183",
    "mgmt_port": 10403,
    "sync_mode": 1,
    "saml_role": "identity-provider",
    "admin_port": 443,
    "serial": "FGVM01TM19000001",
    "host_name": "admin-root",
    "firmware_version_major": 6,
    "firmware_version_minor": 2,
    "firmware_version_patch": 0,
    "firmware_version_build": 1010,
    "subtree_members": [
      {
```

```

        "serial": "FGVM01TM19000002"
    },
    {
        "serial": "FGVM01TM19000003"
    },
    {
        "serial": "FGVM01TM19000004"
    },
    {
        "serial": "FGVM01TM19000005"
    }
]
},
{
    "path": "FGVM01TM19000001:FGVM01TM19000002",
    "mgmt_ip_str": "104.196.102.183",
    "mgmt_port": 10423,
    "sync_mode": 1,
    "saml_role": "service-provider",
    "admin_port": 443,
    "serial": "FGVM01TM19000002",
    "host_name": "Branch_Office_01",
    "firmware_version_major": 6,
    "firmware_version_minor": 2,
    "firmware_version_patch": 0,
    "firmware_version_build": 1010,
    "upstream_intf": "Branch-HQ-A",
    "upstream_serial": "FGVM01TM19000001",
    "parent_serial": "FGVM01TM19000001",
    "parent_hostname": "admin-root",
    "upstream_status": "Authorized",
    "upstream_ip": 22569994,
    "upstream_ip_str": "10.100.88.1",
    "subtree_members": [
    ],
    "is_discovered": true,
    "ip_str": "10.0.10.2",
    "downstream_intf": "To-HQ-A",
    "idx": 1
},
{
    "path": "FGVM01TM19000001:FGVM01TM19000003",
    "mgmt_ip_str": "104.196.102.183",
    "mgmt_port": 10407,
    "sync_mode": 1,
    "saml_role": "service-provider",
    "admin_port": 443,
    "serial": "FGVM01TM19000003",
    "host_name": "Enterprise_Second_Floor",
    "firmware_version_major": 6,
    "firmware_version_minor": 2,
    "firmware_version_patch": 0,
    "firmware_version_build": 1010,
    "upstream_intf": "port3",
    "upstream_serial": "FGVM01TM19000001",
    "parent_serial": "FGVM01TM19000001",

```

```

    "parent_hostname":"admin-root",
    "upstream_status":"Authorized",
    "upstream_ip":22569994,
    "upstream_ip_str":"10.100.88.1",
    "subtree_members":[
    ],
    "is_discovered":true,
    "ip_str":"10.100.88.102",
    "downstream_intf":"port1",
    "idx":2
  },
  {
    "path":"FGVM01TM19000001:FGVM01TM19000004",
    "mgmt_ip_str":"104.196.102.183",
    "mgmt_port":10424,
    "sync_mode":1,
    "saml_role":"service-provider",
    "admin_port":443,
    "serial":"FGVM01TM19000004",
    "host_name":"Branch_Office_02",
    "firmware_version_major":6,
    "firmware_version_minor":2,
    "firmware_version_patch":0,
    "firmware_version_build":1010,
    "upstream_intf":"HQ-MPLS",
    "upstream_serial":"FGVM01TM19000001",
    "parent_serial":"FGVM01TM19000001",
    "parent_hostname":"admin-root",
    "upstream_status":"Authorized",
    "upstream_ip":22569994,
    "upstream_ip_str":"10.100.88.1",
    "subtree_members":[
    ],
    "is_discovered":true,
    "ip_str":"10.0.12.3",
    "downstream_intf":"To-HQ-MPLS",
    "idx":3
  },
  {
    "path":"FGVM01TM19000001:FGVM01TM19000005",
    "mgmt_ip_str":"104.196.102.183",
    "mgmt_port":10404,
    "sync_mode":1,
    "saml_role":"service-provider",
    "admin_port":443,
    "serial":"FGVM01TM19000005",
    "host_name":"Enterprise_First_Floor",
    "firmware_version_major":6,
    "firmware_version_minor":2,
    "firmware_version_patch":0,
    "firmware_version_build":1010,
    "upstream_intf":"port3",
    "upstream_serial":"FGVM01TM19000001",
    "parent_serial":"FGVM01TM19000001",
    "parent_hostname":"admin-root",
    "upstream_status":"Authorized",

```

```
"upstream_ip":22569994,
"upstream_ip_str":"10.100.88.1",
"subtree_members":[
],
"is_discovered":true,
"ip_str":"10.100.88.101",
"downstream_intf":"port1",
"idx":4
}
]
```

Diagnosing automation stitches

Diagnose commands are available to:

- Test an automation stitch
- Enable or disable log dumping for automation stitches
- Display the settings of every automation stitch
- Display statistics on every automation stitch

To test an automation stitch:

```
diagnose automation test <automation-stitch-name>
```

Example:

```
# diagnose automation test HA-failover
automation test is done. stitch:HA-failover
```

To toggle log dumping:

```
diagnose test application autod 1
```

Examples:

```
# diagnose test application autod 1
autod log dumping is enabled

# diagnose test application autod 1
autod log dumping is disabled

autod logs dumping summary:
autod dumped total:7 logs, num of logids:4
```

To display the settings for all of the automation stitches:

```
diagnose test application autod 2
```

Example:

```
# diagnose test application autod 2
csf: enabled root:yes
total stitches activated: 3

stitch: Compromised-IP-Banned
destinations: all
```

```
trigger: Compromised-IP-Banned

local hit: 0 relayed to: 0 relayed from: 0
actions:
    Compromised-IP-Banned_ban-ip type:ban-ip interval:0

stitch: HA-failover
destinations: HA-failover_ha-cluster_25;
trigger: HA-failover

local hit: 0 relayed to: 0 relayed from: 0
actions:
    HA-failover_email type:email interval:0
    subject: HA Failover
    mailto:admin@example.com;

stitch: reboot
destinations: all
trigger: reboot

local hit: 0 relayed to: 0 relayed from: 0
actions:
    action1 type:alicloud-function interval:0
        delay:1 required:yes
        Account ID: id
        Region: region
        Function domain: fc.aliyuncs.com
        Version: versoin
        Service name: serv
        Function name: funky
        headers:
```

To display statistic on all of the automation stitches:

```
diagnose test application autod 3
```

Example:

```
# diagnose test application autod 3
stitch: Compromised-IP-Banned
local hit: 0 relayed to: 0 relayed from: 0
last trigger:Wed Dec 31 20:00:00 1969
last relay:Wed Dec 31 20:00:00 1969
actions:
    Compromised-IP-Banned_ban-ip:
        done: 1 relayed to: 0 relayed from: 0
        last trigger:Wed Dec 31 20:00:00 1969
        last relay:

stitch: HA-failover
local hit: 0 relayed to: 0 relayed from: 0
last trigger:Thu May 24 11:35:22 2018
last relay:Thu May 24 11:35:22 2018
actions:
    HA-failover_email:
        done: 1 relayed to: 1 relayed from: 1
        last trigger:Thu May 24 11:35:22 2018
```

```
last relay:Thu May 24 11:35:22 2018

stitch: reboot
  local hit: 2 relayed to: 1 relayed from: 1
  last trigger:Fri May 3 13:30:56 2019
  last relay:Fri May 3 13:30:23 2019
  actions:
    action1
      done: 1 relayed to: 0 relayed from: 0
      last trigger:Fri May 3 13:30:56 2019
      last relay:

logid2stitch mapping:
id:20103 local hit: 0 relayed to: 0 relayed from: 0
  License Expiry
  lambada

id:32138 local hit: 2 relayed to: 1 relayed from: 1
  Compromised-IP-Banned
  HA-failover
  reboot

action run cfg&stats:
total:2 cur:0 done:1 drop:1
email:
  flags:10
  stats: total:1 cur:0 done:1 drop:0
ios-notification:
  flags:1
  stats: total:0 cur:0 done:0 drop:0
alert:
  flags:0
  stats: total:0 cur:0 done:0 drop:0
disable-ssid:
  flags:7
  stats: total:0 cur:0 done:0 drop:0
quarantine:
  flags:7
  stats: total:0 cur:0 done:0 drop:0
quarantine-forticlient:
  flags:4
  stats: total:0 cur:0 done:0 drop:0
quarantine-nsx:
  flags:4
  stats: total:0 cur:0 done:0 drop:0
ban-ip:
  flags:7
  stats: total:0 cur:0 done:0 drop:0
aws-lambda:
  flags:11
  stats: total:0 cur:0 done:0 drop:0
webhook:
  flags:11
  stats: total:0 cur:0 done:0 drop:0
cli-script:
  flags:10
```



```
stats: total:0 cur:0 done:0 drop:0
azure-function:
  flags:11
  stats: total:1 cur:0 done:0 drop:1
google-cloud-function:
  flags:11
  stats: total:0 cur:0 done:0 drop:0
alicloud-function:
  flags:11
  stats: total:0 cur:0 done:0 drop:0
```

FortiView

FortiView is the FortiOS log view tool which is a comprehensive monitoring system for your network. FortiView integrates real-time and historical data into a single view on your FortiGate. It can log and monitor network threats, filter data on multiple levels, keep track of administration activities, and more.

You can use multiple filters in the consoles to narrow your view to a specific time range, by user ID or local IP address, by application, and many more.

Use FortiView to investigate traffic activity such as user uploads/downloads or videos watched on YouTube. You view the traffic on the whole network, by user group, or by individual. FortiView displays the information in both text and visual format, giving you an overall picture of your network traffic activity so that you can quickly decide on actionable items.

Logging range and depth depends on the FortiGate model.

The following are just some of the FortiView categories:

- | | | | |
|---------------------|---------------------------------|----------------|--------------------------|
| • Sources | • Web Sites | • Admin Login | • WiFi Clients |
| • Destinations | • Threats | • VPN Login | • Threat Map |
| • Applications | • All Sessions | • FortiSandbox | • Traffic Shaping |
| • Cloud Application | • Failed Authentication Attempt | • Policy | • Endpoint Vulnerability |
| • Country | • System Events | • Interface | |

FortiOS has widgets that you can use to further customize these categories. You can place widgets where you want on dashboards. You can also customize widgets to show information that is most important to you, such as the time range, source logging device, and other information.

FortiView is integrated with many UTM functions and each release adds more features. For example, you can quarantine an IP address directly in FortiView or create custom devices and addresses from a FortiView entry.

FortiView interface

FortiView dashboards allow you to access information about traffic activity on your FortiGate, visually and textually. Core FortiView dashboards, including *Sources*, *Destinations*, *Applications* and more are available within the FortiView tree menu, and include a top menu bar with the following features:

- A *refresh* button which updates the displayed data.
- A *time display* dropdown for switching between current and historical data.
- An *Add Filter* button for applying filters to the displayed data.
- A *view selection* dropdown for changing what information shown on the dashboard.



Additional FortiView information is available as widgets to be placed within default or custom dashboards in the *Dashboard* menu. See [FortiView dashboards and widgets on page 305](#).

Time display

Using the *time display* dropdown, you can select the time period to be displayed on the current dashboard. Time display options vary depending on the dashboard and can include current information (*now*) and historical information (*1 hour*, *24 hours*, and *7 days*).



In order to view historical information, disk logging must be enabled.

FortiView filters

You can filter FortiView dashboards by using the *Add Filter* box in the toolbar and selecting a context-sensitive filter. Available filters vary depending on the FortiView dashboard.

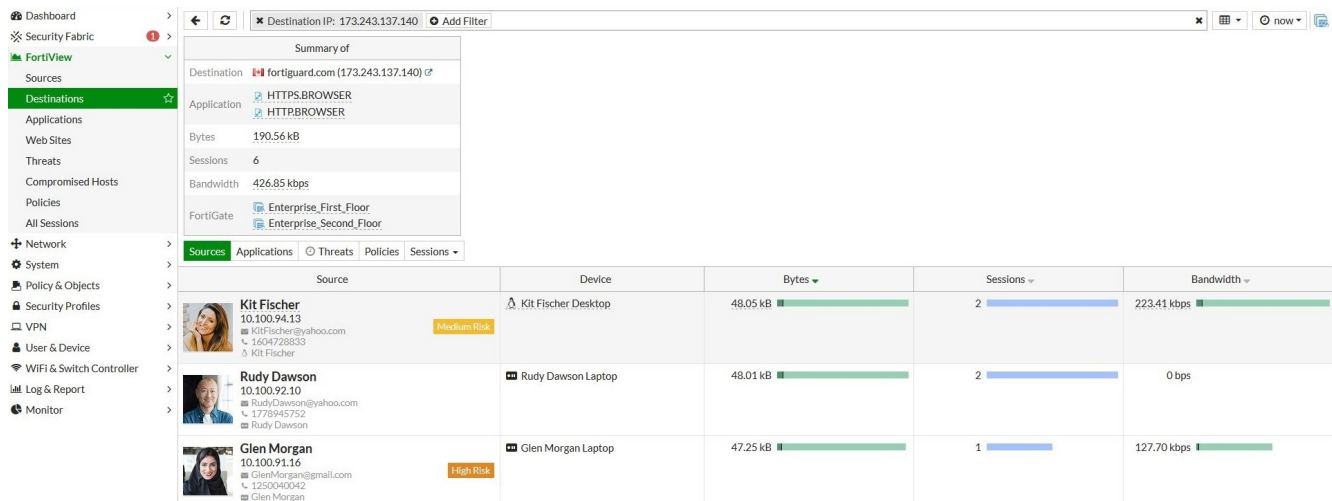
To filter results on a FortiView dashboard:

1. Select a dashboard in FortiView.
2. Click *Add Filter* in the dashboard toolbar.
3. Select a filter from the available list.
Available filters are presented for quick selection. Additional filters can be added by clicking the *Add Filter* button in the toolbar again.

Dashboard	Country/Region: Canada	Destination Device	Application	Bytes	Sessions	Bandwidth
Security Fabric	Destination IP	FortiGate				
FortiView	Sources	ntp2.fortiguards.com (208.91.114.23)		749.74 kB	2	848 bps
	Destinations	ntp1.fortinet.net (208.91.113.70)	NTP	658.39 kB	3	1.06 kbps
	Applications	ntp2.fortiguards.com (208.91.113.71)	NTP	638.40 kB	1	424 bps
	Web Sites	ntp1.fortiguards.com (208.91.113.222)	NTP	543.40 kB	2	0 bps
	Threats	208.91.112.220	Fortinet-FortiGuard	153.95 kB	327	58.91 kbps
	Compromised Hosts	usfgd1.fortiguards.com (173.243.138.200)	HTTPS.BROWSER	23.90 kB	1	0 bps
	Policies	173.243.138.221	Fortinet-FortiGuard	8.32 kB	26	2.24 kbps
	All Sessions	173.243.138.194	Fortiguards.Search	0 B	11	0 bps

Drill down to details

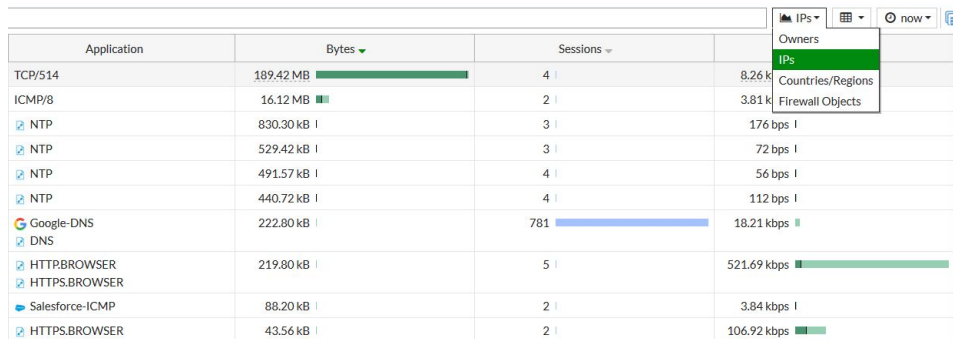
Double-click or right-click on an entry in a FortiView dashboard and select *Drill Down to Details* to view additional details about the selected traffic activity. Click the *back* icon in the toolbar to return to the previous view. *Drill down to details* is not available on the *All Sessions* dashboard.



View selection

Selecting which information is shown:

Most FortiView pages include multiple views for displaying different types of information. You can switch between views by clicking the dropdown in the top menu bar and choosing a view.



Selecting a display type:

Display types include table view, bubble charts, and country maps. Not all display types are supported by all dashboards in FortiView. On pages that support multiple displays, select the icon in the top-right corner of the dashboard to choose a display.

- In the default table view, you can customize the columns that are displayed by hovering your mouse over the first column header and clicking the *configure table* icon.
- When using a bubble chart, it is possible to sort information using the *Compare By* dropdown menu. The size of each bubble represents the related amount of data. You can place your cursor over a bubble to display a tool-tip with detailed information on that item, and click on a bubble to drilldown into greater (filtered) detail.

FortiView from disk

Prerequisites

All FortiGates with an SSD disk.

Restrictions

- Desktop models (for example: under 100D) with SSD only supports five minutes and one hour view.
- Medium models (for example: 200D, 500D) with SSD supports up to 24 hours view.
- Large models (for example: 1500D and above) with SSD supports up to seven days view.
 - To enable seven days view:

```
config log setting
    set fortiview-weekly-data enable
end
```

Configuration

A firewall policy needs to be in place with traffic logging enabled. For best operation with FortiView, internal interface roles should be clearly defined as LAN; DMZ and internet facing or external interface roles should be defined as WAN.

To enable FortiView from Disk:

1. Enable disk logging from the FortiGate GUI.
 - a. Go to *Log & Report > Log Settings > Local Log*.
 - b. Select the checkbox next to *Disk*.
2. Enable historical FortiView from the FortiGate GUI.
 - a. Go to *Log & Report > Log Settings > Local Log*.
 - b. Select the checkbox next to *Enable Historical FortiView*.

Log Settings

Local Log

- | | |
|-----------------------------|-------------------------------------|
| Disk | <input checked="" type="checkbox"/> |
| Enable Local Reports | <input type="checkbox"/> |
| Enable Historical FortiView | <input checked="" type="checkbox"/> |

3. Click *Apply*.

To include sniffer traffic and local-deny traffic when FortiView from Disk:

This feature is only supported through the CLI.

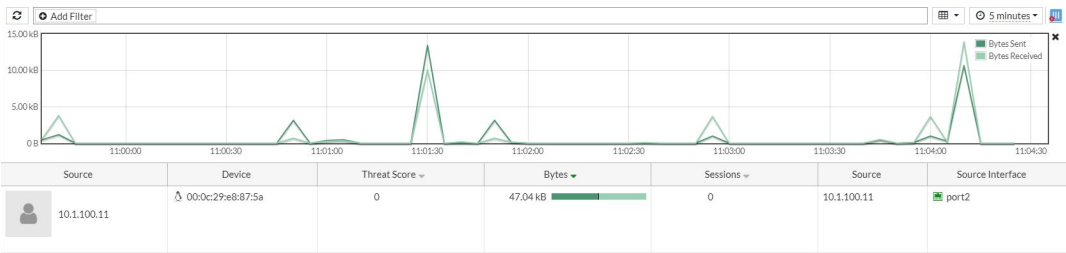
```
config report setting
    set report-source forward-traffic sniffer-traffic local-deny-traffic
```

end

Source View

Top Level

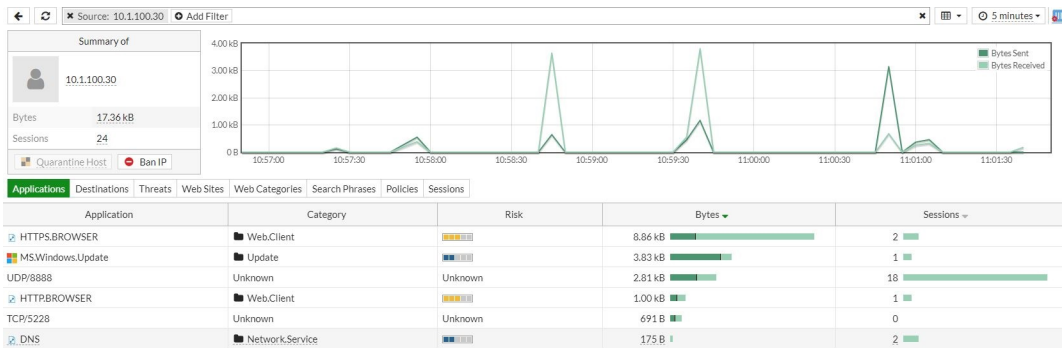
Sample entry:



Time	<ul style="list-style-type: none">Realtime or <i>Now</i> entries are determined by the FortiGate's system session list.Historical or <i>5 minutes and later</i> entries are determined by traffic logs, with additional information coming from UTM logs.
Graph	<ul style="list-style-type: none">The graph shows the bytes sent/received in the time frame. Realtime does not include a chart.Users can customize the time frame by selecting a time period within the graph.
Bubble Chart	<ul style="list-style-type: none">Bubble chart shows the same information as the table, but in a different graphical manner.
Columns	<ul style="list-style-type: none"><i>Source</i> shows the IP address (and user as well as user avatar if configured) of the source device.<i>Device</i> shows the device information as listed in <i>User & Device > Device Inventory</i>. Device detection should be enabled on the applicable interfaces for best function.<i>Threat Score</i> is the threat score of the source based on UTM features such as Web Filter and antivirus. It shows threat scores allowed and threat scores blocked.<i>Bytes</i> is the accumulated bytes sent/received. In realtime, this is calculated from the session list, and in historical it is from logs.<i>Sessions</i> is the total sessions blocked/allowed. In realtime, this is calculated from the session list, and in historical it is from logs.<i>Source</i> is a simplified version of the first column, including only the IP address without extra information.<i>Source Interface</i> is the interface from which the traffic originates. In realtime, this is calculated from the session list, and in historical it is from the logs.More information can be shown in a tooltip while hovering over these entries.For realtime, two more columns are available, <i>Bandwidth</i> and <i>Packets</i>, both of which come from the session list.

Drilldown Level

Sample entry:



Graph

- The graph shows the bytes sent/received in the time frame. Realtime does not include a chart.
- Users can customize the time frame by selecting a time period within the graph.

Summary Information

- Shows information such as the user/avatar, avatar/source IP, bytes, and sessions total for the time period.
- Can quarantine host (access layer quarantine) if they are behind a FortiSwitch or FortiAP.
- Can ban IP addresses, adds the source IP address into the quarantine list.

Tabs

- Drilling down entries in any of these tabs (except sessions tab) will take you to the underlying traffic log in the sessions tab.
- Applications** shows a list of the applications attributed to the source IP. This can include scanned applications (using Application Control in a firewall policy or unscanned applications).


```
config log gui-display
    set fortiview-unscanned-apps enable
end
```
- Destinations** shows destinations grouped by IP address/FQDN.
- Threats** lists the threats caught by UTM profiles. This can be from antivirus, IPS, Web Filter, Application Control, etc.
- Web Sites** contains the websites which were detected either with webfilter, or through FQDN in traffic logs.
- Web Categories** groups entries into their categories as dictated by the Web Filter Database.
- Search Phrases** shows entries of search phrases on search engines captured by a Web Filter UTM profile, with deep inspection enabled in firewall policy.
- Policies** groups the entries into which policies they passed through or were blocked by.
- Sessions** shows the underlying logs (historical) or sessions (realtime). Drilldowns from other tabs end up showing the underlying log located in this tab.
- More information can be shown in a tooltip while hovering over these entries.

Troubleshooting

- Use `diagnose debug application httpsd -1` to check which filters were passed through httpsd. For example:


```
[httpsd 3163 - 1546543360 info] api_store_parameter[227] -- add API parameter
'filter': '{ "source": "10.1.100.30", "application": "TCP/5228", "srcintfrole":
[ "lan", "dmz", "undefined" ] }' (type=object)
```

- Use `diagnose debug application miglogd 0x70000` to check what the SQL command is that is passed to the underlying SQL database.

For example:

```
fortiview_request_data()-898: total:31 start:1546559580 end:1546563179
_dump_sql()-799: dataset=fv.general.chart, sql:select a.timestamp1,ses_al,ses_
bk,r,s,ifnull(sc_l,0),ifnull(sc_m,0),ifnull(sc_h,0),ifnull(sc_c,0) from (select
timestamp-(timestamp%60) timestamp1 ,sum(case when passthrough<>'block' then
sessioncount else 0 end) ses_al,sum(case when passthrough='block' then
sessioncount else 0 end) ses_bk,sum(rcvdbyte) r,sum(sentbyte) s from grp_
traffic_all_src where timestamp BETWEEN 1546559580 and 1546563179 and l=1 AND
srcip in ('10.1.100.11') AND srcintfrole in ('lan','dmz','undefined') group by
timestamp1 ) a left join (select timestamp-(timestamp%60) timestamp1 ,sum(case
when threat_level=1 then crscore else 0 end) sc_l,sum(case when threat_level=2
then crscore else 0 end) sc_m,sum(case when threat_level=3 then crscore else 0
end) sc_h,sum(case when threat_level=4 then crscore else 0 end) sc_c from grp_
threat where timestamp BETWEEN 1546559580 and 1546563179 and l=1 AND srcip in
('10.1.100.11') AND srcintfrole in ('lan','dmz','undefined') group by timestamp1
) b on a.timestamp1 = b.timestamp1;
takes 40(ms), aggr:0(ms)
```

- Use `execute report flush-cache` and `execute report recreate-db` to clear up any irregularities that may be caused by upgrading or cache issues.

FortiView from FortiAnalyzer

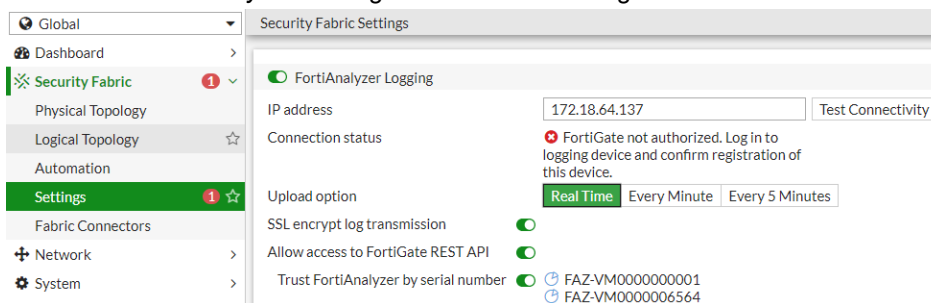
Attaching a FortiAnalyzer to the FortiGate increases the functionality of *FortiView*. For example, it adds the *Compromised Hosts* view.

The following devices are required:

- A FortiGate or FortiOS
- A compatible FortiAnalyzer (see <https://docs.fortinet.com/document/fortianalyzer/6.2.0/compatibility-with-fortios>)

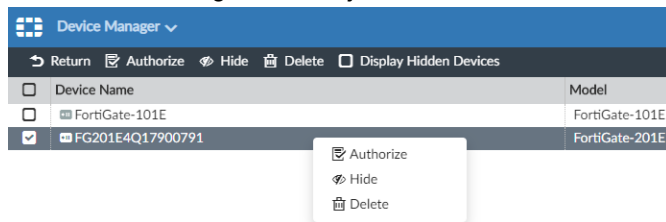
To enable FortiView from FortiAnalyzer:

1. On the FortiGate, go to *Security Fabric > Settings*.
2. Turn on *FortiAnalyzer Logging* and enter the IP address of the FortiAnalyzer device.
3. Click *Test Connectivity*. A message will be shown stating that the FortiGate is not authorized on the FortiAnalyzer.

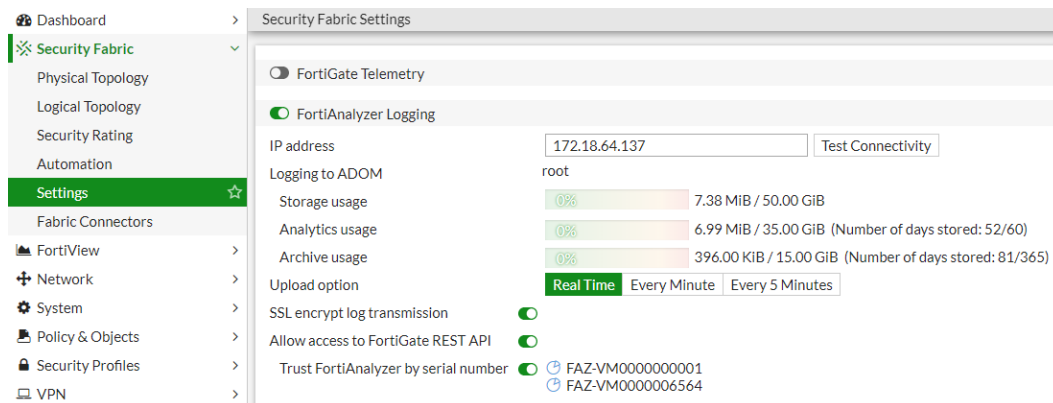


4. On the FortiAnalyzer, go to *Device Manager*.

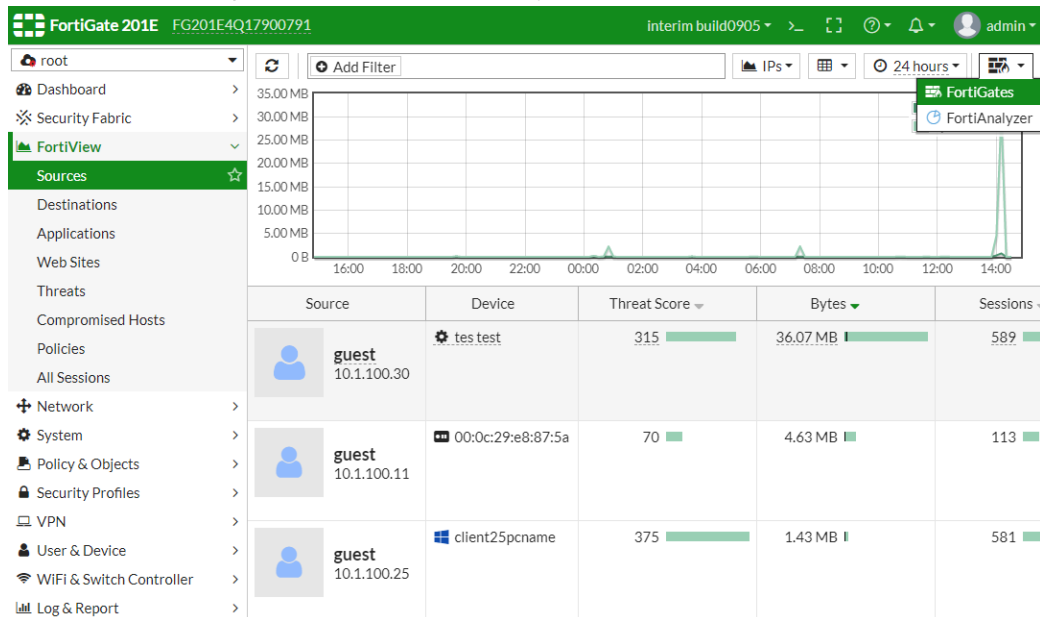
5. In the device list, right click the just added FortiGate, then click *Authorize*.



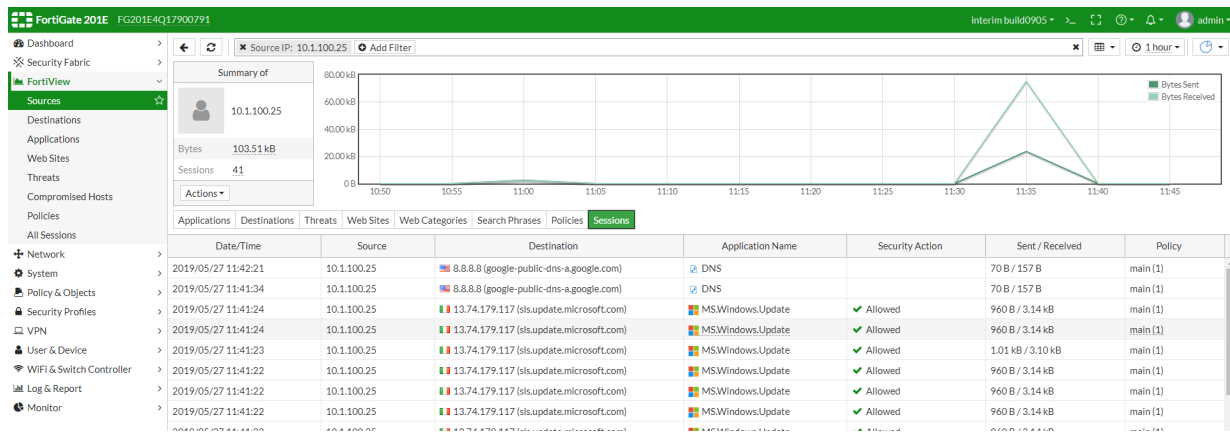
6. On the FortiGate, go to *Security Fabric > Settings* and click Test Connectivity to confirm that the device is now authorized.



7. Go to *FortiView > Sources*.
8. Select a time range other than *now* from the drop-down list to view historical data.
9. From the source drop-down list, select *FortiAnalyzer*.



All the historical information now comes from the FortiAnalyzer.



Cloud application view

To see different cloud application views, set up the following:

- A FortiGate having a relative firewall policy with the Application Control security profile.
- A FortiGate with log data from the local disk or FortiAnalyzer.
- Optional but highly recommended: *SSL Inspection* set to *deep-inspection* on relative firewall policies.

Viewing cloud applications

Cloud applications

All cloud applications require *SSL Inspection* set to *deep-inspection* on the firewall policy. For example, *Facebook_File.Download* can monitor Facebook download behavior which requires *SSL deep-inspection* to parse the deep information in the network packets.

To view cloud applications:

1. Go to *Security Profiles > Application Control*.
2. Edit a profile that is used by the firewall policy.

3. On the *Edit Application Sensor* page, click *View Application Signatures*.

FortiGate 401E FGT_A

root

Edit Application Sensor

97 Cloud Applications require deep inspection.
1 policies are using this profile.

Name: g-Clone of g-default

Comments: Monitor all applications. 25/255

View Application Signatures

Categories

All Categories

- Business (142, 6)
- Game (83)
- P2P (58)
- Storage.Backup (162, 17)
- Web.Client (23)
- Cloud.IT (47)
- General.Interest (225, 7)
- Proxy (170)
- Update (49)
- Unknown Applications
- Collaboration (256, 10)
- Mobile (3)
- Remote.Access (82)
- Video/Audio (150, 14)
- Email (78, 12)
- Network.Service (330)
- Social.Media (119, 31)
- VoIP (24)

Network Protocol Enforcement

Application and Filter Overrides

View

Priority	Details	Type	Action
No results			

Options

Allow and Log DNS Traffic ☒

QUIC ☒ Allow Block

Replacement Messages for HTTP-based Applications ☒

Return

4. On the top right of the *Application Signature* page, click *Cloud* to display all cloud signature based applications. Cloud applications have a cloud icon beside them.

The lock icon indicates that that application requires SSL deep inspection.

Application Signature					
Name	Category	Technology	Popularity	Risk	Behavior
Amazon.Cloud.Drive.File.Download	Storage.Backup	Browser-Based	★★★★☆	Low	Excessive-Bandwidth Cloud
Amazon.Cloud.Drive.File.Upload	Storage.Backup	Browser-Based	★★★★☆	Low	Excessive-Bandwidth Cloud
Box.File.Download	Storage.Backup	Browser-Based	★★★★☆	Low	Excessive-Bandwidth Cloud
Box.File.Upload	Storage.Backup	Browser-Based	★★★★☆	Low	Excessive-Bandwidth Cloud
Dropbox.File.Download	Storage.Backup	Browser-Based	★★★★☆	Low	Excessive-Bandwidth Cloud
Dropbox.File.Upload	Storage.Backup	Browser-Based	★★★★☆	Low	Excessive-Bandwidth Cloud
Evernote.File.Download	General.Interest	Browser-Based	★★★★★	Low	Excessive-Bandwidth Cloud
Evernote.File.Upload	General.Interest	Browser-Based	★★★★★	Low	Excessive-Bandwidth Cloud
Facebook.File.Download	Social.Media	Browser-Based	★★★★☆	Low	Excessive-Bandwidth Cloud
Facebook.File.Upload	Social.Media	Browser-Based	★★★★☆	Low	Excessive-Bandwidth Cloud
Flickr.File.Upload	Social.Media	Browser-Based	★★★★☆	Low	Excessive-Bandwidth Cloud
Foursquare.File.Upload	Social.Media	Browser-Based	★★★★★	Low	Excessive-Bandwidth Cloud
Gmail.Attachment.Download	Email	Browser-Based	★★★★☆	Low	Excessive-Bandwidth Cloud
Gmail.Attachment.Upload	Email	Browser-Based	★★★★☆	Low	Excessive-Bandwidth Cloud
Google.Docs.File.Download	Collaboration	Browser-Based	★★★★☆	Low	Excessive-Bandwidth Cloud
Google.Docs.File.Upload	Collaboration	Browser-Based	★★★★☆	Low	Excessive-Bandwidth Cloud
Google.Drive.File.Download	Storage.Backup	Browser-Based	★★★★☆	Low	Excessive-Bandwidth Cloud
Google.Drive.File.Upload	Storage.Backup	Browser-Based	★★★★☆	Low	Excessive-Bandwidth Cloud
Google.Plus.File.Upload	Social.Media	Browser-Based	★★★★☆	Low	Excessive-Bandwidth Cloud

5. Hover over an item to see its details.

This example shows the *Gmail_Attachment.Download*, a cloud application signature based sensor which requires SSL deep inspection. If any local network user behind the firewall logs into Gmail and downloads a Gmail attachment, that activity is logged.

Name	Category
Box.File.Download	Storage.Backup
Box.File.Upload	
Dropbox.File.Download	
Dropbox.File.Upload	
Evernote.File.Download	
Evernote.File.Upload	
Facebook.File.Download	
Facebook.File.Upload	
Flickr.File.Upload	
Foursquare.File.Upload	
Gmail.Attachment.Download	Email

Gmail.Attachment.Download

ID: 38726

Summary: This indicates an attempt to download an attachment from Gmail. Gmail Attachment Download detects and logs the name of the file downloaded by the user in an email message.

Information Displayed: User's IP/Username/Email Address depending on traffic

File Name

Category: Email

Risk: Low

Popularity: ★★★★★

Protocol: TCP, HTTP

Technology: Browser-Based

Behavior: Excessive-Bandwidth, Cloud

Vendor: Google

Legend: Cloud Application, Requires SSL Deep Inspection

Applications with cloud behavior

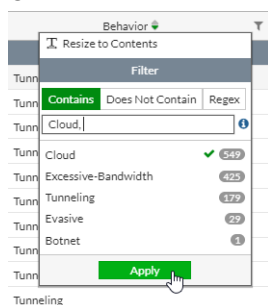
Applications with cloud behavior is a superset of cloud applications.

Some applications do not require SSL deep inspection, such as Facebook, Gmail, YouTube, and so on. This means that if any traffic trigger application sensors for these applications, there is a FortiView cloud application view for that traffic.

Other applications require SSL deep inspection, such as Gmail attachment, Facebook_Workplace, and so on.

To view applications with cloud behavior:

1. On the *Application Signature* page, add the *Behavior* column if it is not already visible:
 - a. Hover over the left of the table column headings to display the *Configure Table* icon.
 - b. Click *Configure Table* and select *Behavior*.
 - c. Click *Apply*.
2. Click the Filter icon in the *Behavior* column and enter *Cloud* to filter by Cloud, then click *Apply*.



3. The *Application Signature* page displays all applications with cloud behavior.

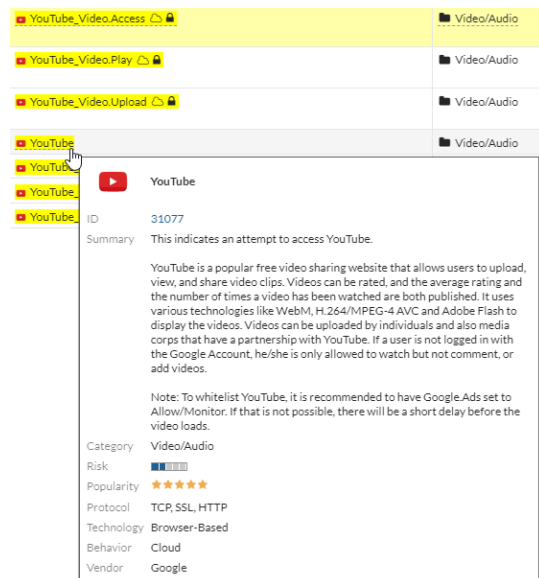
+ Create New	Edit	Delete	Search	Q	All	Cloud
Name	Category	Technology	Popularity	Risk	Behavior	
Application Signature 549/2092						
4shared_File.Download	Storage.Backup	Browser-Based Client-Server	★★★★☆	■■■■■	Excessive-Bandwidth Cloud	
4shared_File.Upload	Storage.Backup	Browser-Based Client-Server	★★★★☆	■■■■■	Excessive-Bandwidth Cloud	
360.Yunpan_File.Download	Storage.Backup	Browser-Based Client-Server	★★☆☆☆	■■■■■	Excessive-Bandwidth Cloud	
360.Yunpan_File.Upload	Storage.Backup	Browser-Based Client-Server	★★★★☆	■■■■■	Excessive-Bandwidth Cloud	
Acrobat.Cloud.Download	Storage.Backup	Browser-Based	★★☆☆☆	■■■■■	Excessive-Bandwidth Cloud	
Acrobat.Cloud.Upload	Storage.Backup	Browser-Based	★★★★☆	■■■■■	Excessive-Bandwidth Cloud	
ActiveCampaign_File.Upload	Business	Browser-Based	★★★★☆	■■■■■	Excessive-Bandwidth Cloud	
Adobe.Connect_Meeting.Share.Document.Upload	Collaboration	Browser-Based	★★★★☆	■■■■■	Excessive-Bandwidth Cloud	
Adobe.Creative.Cloud_File.Download	Storage.Backup	Browser-Based	★★☆☆☆	■■■■■	Excessive-Bandwidth Cloud	
Adobe.Creative.Cloud_File.Upload	Storage.Backup	Browser-Based	★★☆☆☆	■■■■■	Excessive-Bandwidth Cloud	
Amazon.Cloud.Drive_File.Download	Storage.Backup	Browser-Based	★★★★☆	■■■■■	Excessive-Bandwidth Cloud	
Amazon.Cloud.Drive_File.Upload	Storage.Backup	Browser-Based	★★★★☆	■■■■■	Excessive-Bandwidth Cloud	
AutoDesk.360.Upload	Business	Browser-Based	★★★★☆	■■■■■	Excessive-Bandwidth Cloud	
Backblaze_Restore	Storage.Backup	Browser-Based Client-Server	★★★★☆	■■■■■	Excessive-Bandwidth Cloud	
Baidu.Cloud_File.Download	Storage.Backup	Browser-Based	★★★★☆	■■■■■	Excessive-Bandwidth Cloud	
Baidu.Cloud_File.Upload	Storage.Backup	Browser-Based	★★★★☆	■■■■■	Excessive-Bandwidth Cloud	
BambooHR_File.Download	Business	Browser-Based	★★★★☆	■■■■■	Excessive-Bandwidth Cloud	
BambooHR_File.Upload	Business	Browser-Based	★★★★☆	■■■■■	Excessive-Bandwidth Cloud	
Barracuda_Backup	Storage.Backup	Browser-Based	★★☆☆☆	■■■■■	Excessive-Bandwidth Cloud	0% 549/2092

4. Use the Search box to search for applications. For example, you can search for *youtube*.


+ Create New	Edit	Delete	youtube	X	Q	All	Cloud
Name	Category	Technology	Popularity	Risk	Behavior		
Application Signature 7204							
YouTube_Video.Access	Video/Audio	Browser-Based	★★★★☆	■■■■■	Excessive-Bandwidth Cloud		
YouTube_Video.Play	Video/Audio	Browser-Based	★★★★☆	■■■■■	Excessive-Bandwidth Cloud		
YouTube_Video.Upload	Video/Audio	Browser-Based	★★★★☆	■■■■■	Excessive-Bandwidth Cloud		
YouTube	Video/Audio	Browser-Based	★★★★☆	■■■■■	Cloud		
YouTube_Channel.Access	Video/Audio	Browser-Based	★★★★☆	■■■■■	Cloud		
YouTube_Channel.ID	Video/Audio	Browser-Based	★★★★☆	■■■■■	Cloud		
YouTube_Comment.Posting	Video/Audio	Browser-Based	★★☆☆☆	■■■■■	Cloud		

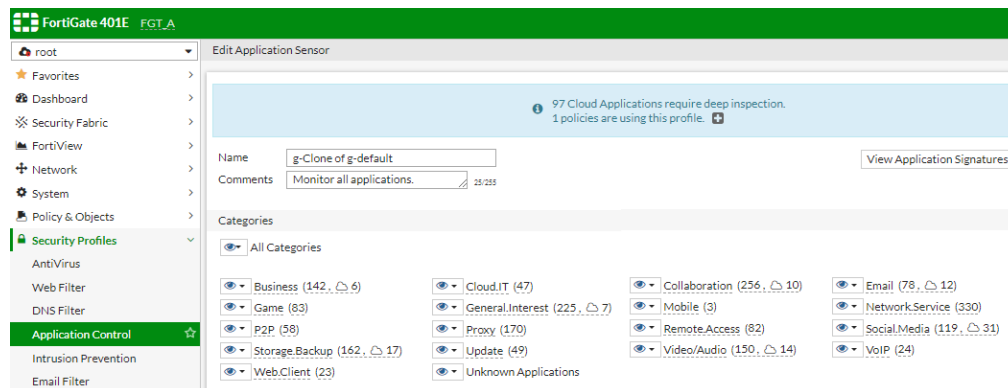
5. Hover over an item to see its details.

This example shows an application sensor with no lock icon which means that this application sensor does not require SSL deep inspection. If any local network user behind the firewall tries to navigate the YouTube website, that activity is logged.



Configuring the Cloud Applications widget

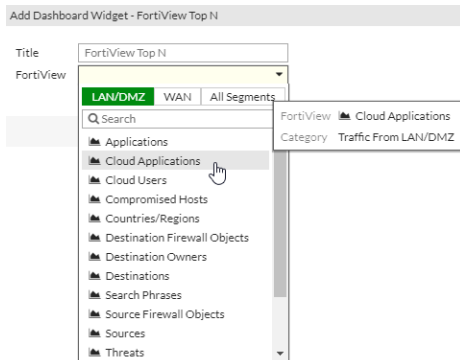
On the *Edit Application Sensor* page in the *Categories* section, the  icon besides a category means that category is monitored and logged.



To add the Cloud Applications widget:

1. Go to *Dashboard > Top Usage LAN/DMZ*.
2. Move the cursor to the bottom right, click the widget control icon and select *Add Widget*.
3. Select *FortiView Top N*.

4. In the *FortiView* dropdown list, select the *LAN/DMZ* tab and then select *Cloud Applications*.



5. Click *Add Widget*.

Top Cloud Applications by Bytes 5 minutes

Application	Category	Risk	Bytes	Sessions	Files (Up/Down)	Videos Played
YouTube	Video/Audio	<div><div></div></div>	7.96 MB	32	0	0
Dropbox	Storage.Backup	<div><div></div></div>	18.38 kB	3	0	0
Facebook	Social.Media	<div><div></div></div>	9.90 kB	2	0	0

6. If SSL deep inspection is enabled on the relative firewall, then the widget shows the additional details that are logged, such as *Files (Up/Down)* and *Videos Played*.

For YouTube, the *Videos Played* column is triggered by the *YouTube_Video.Play* cloud application sensor. This shows the number of local network users who logged into YouTube and played YouTube videos.

For Dropbox, the *Files (Up/Down)* column is triggered by *Dropbox_File.Download* and *Dropbox_File.Upload* cloud application sensors. This shows the number of local network users who logged into Dropbox and uploaded or downloaded files.

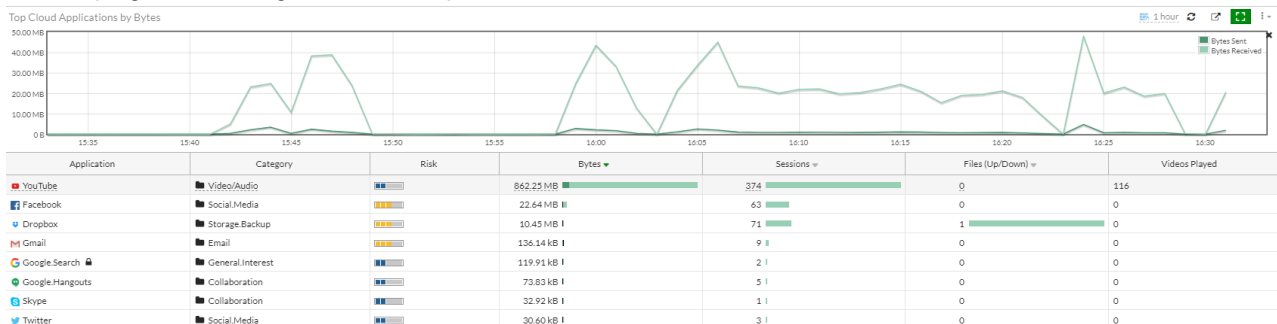
Top Cloud Applications by Bytes 5 minutes

Application	Category	Risk	Bytes	Sessions	Files (Up/Down)	Videos Played
YouTube	Video/Audio	<div><div></div></div>	137.53 MB	120	0	34
Dropbox	Storage.Backup	<div><div></div></div>	7.34 MB	29	1	0
Google.Hangouts	Collaboration	<div><div></div></div>	35.21 kB	3	0	0
Facebook	Social.Media	<div><div></div></div>	33.03 kB	6	0	0
Skype	Collaboration	<div><div></div></div>	32.92 kB	1	0	0

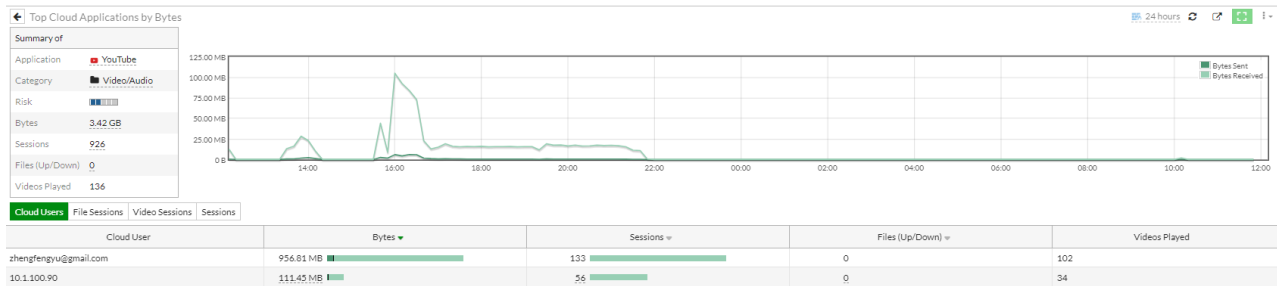
Using the Cloud Applications widget

To see additional information in the Cloud Applications widget:

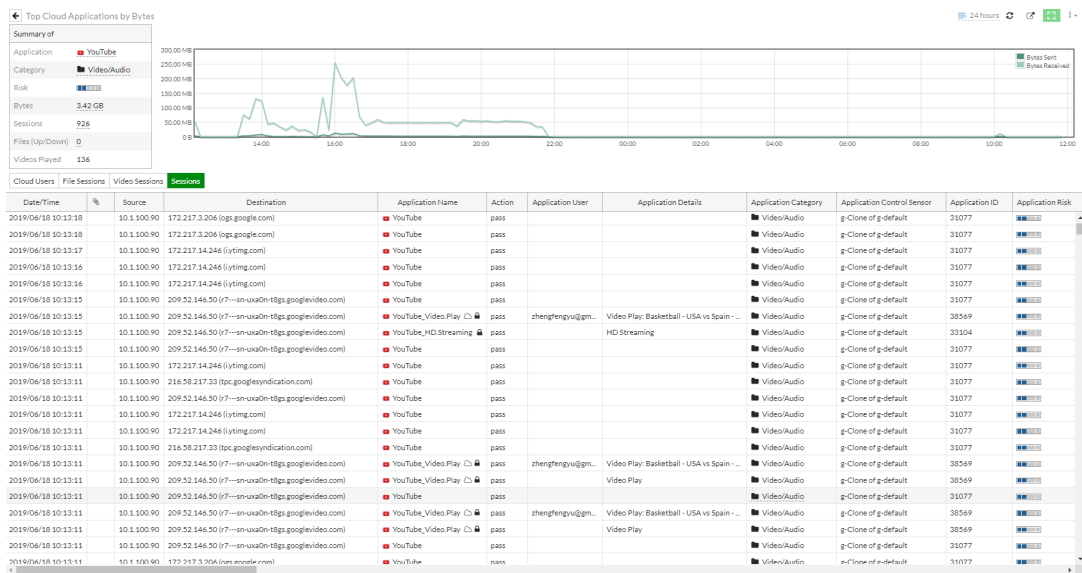
1. In the top right of the widget, click the *Expand to full screen* icon to see additional information.



2. For details about a specific entry, double-click the entry or right-click the entry and select *Drill Down to Details*.



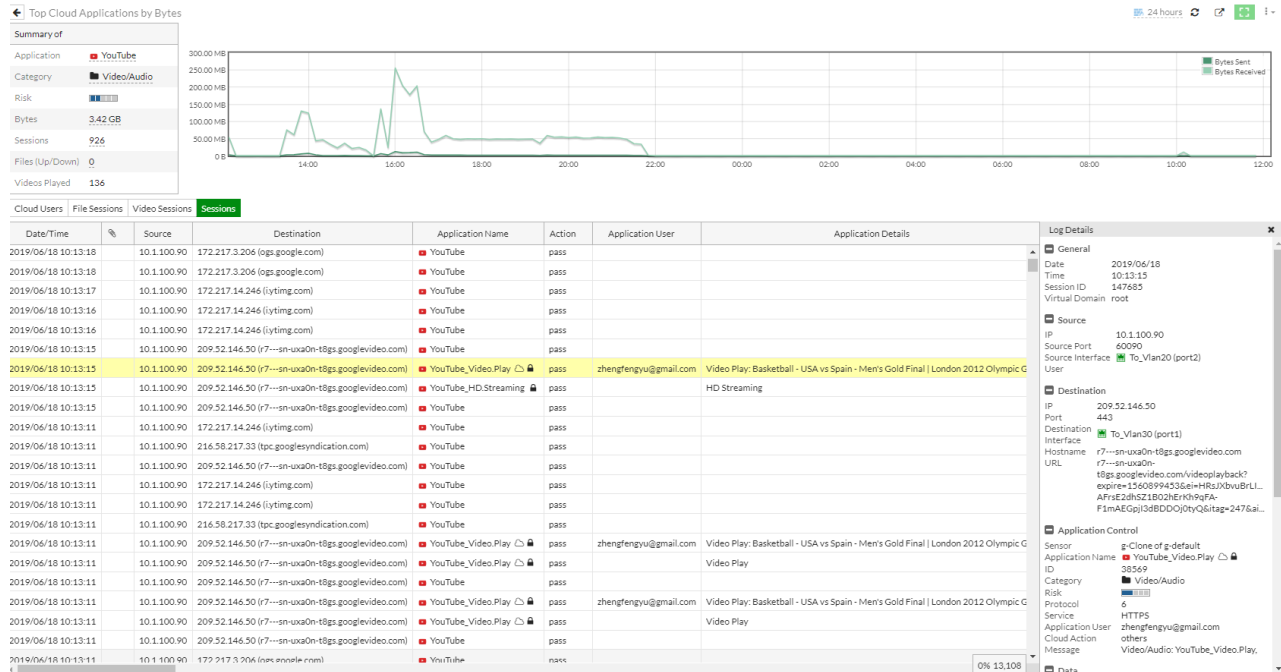
3. To see all the sessions for an application, click *Sessions*.
In this example, the *Application Name* column shows all applications related to YouTube.



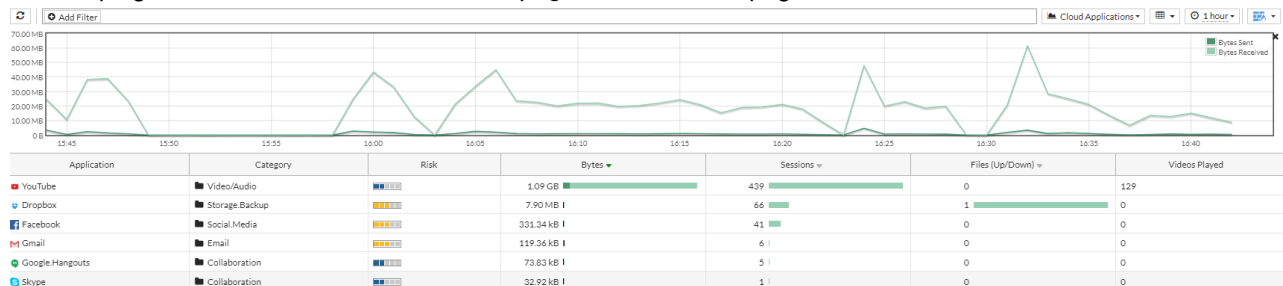
4. To view log details, double-click a session to display the *Log Details* pane.

Sessions monitored by SSL deep inspection (in this example, Youtube_Video.Play) captured deep information such as *Application User*, *Application Details*, and so on. The *Log Details* pane also shows additional deep information such as application *ID*, *Message*, and so on.

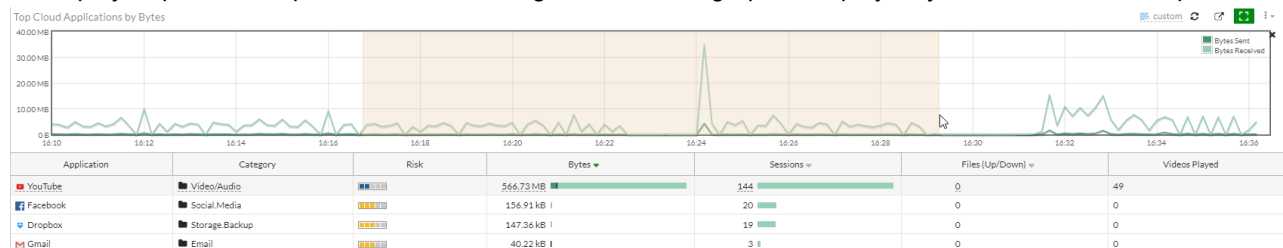
Sessions not monitored by SSL deep inspection (YouTube) did not capture the deep information.



5. In the top right, click the *Standalone FortiView* page icon to see the page in standalone view.



6. To display a specific time period, select and drag in the timeline graph to display only the data for that time period.



Cloud application view examples

Example of monitoring network traffic with SSL deep inspection

This is an example of monitoring network traffic for YouTube via FortiView cloud application view with SSL deep inspection.

To monitor network traffic with SSL deep inspection:

1. Use a firewall policy with the following settings. If necessary, create a policy with these settings.

- *Application Control* is enabled.
- *SSL Inspection* is set to *deep-inspection*.
- *Log Allowed Traffic* is set to *All Sessions*.

Inspection Mode **Flow-based** Proxy-based

Firewall / Network Options

NAT ☒

IP Pool Configuration **Use Outgoing Interface Address** Use Dynamic IP Pool

Preserve Source Port ☐

Protocol Options **PRX** default

Security Profiles

AntiVirus ☐

Web Filter ☐

DNS Filter ☐

Application Control ☒ **APP** g-Clone of g-default

IPS ☒ **IPS** g-Clone of g-default

VoIP ☐

SSL Inspection ☒ **SSL** deep-inspection

Mirror SSL Traffic to Interfaces ☐

Logging Options

Log Allowed Traffic ☒ Security Events **All Sessions**

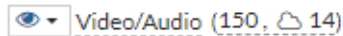
Capture Packets ☐

Comments 0/1023

Enable this policy ☒

2. Go to *Security Profiles > Application Control*.
3. Select a relative Application Control profile used by the firewall policy and click *View*.

4. Because YouTube cloud applications are categorized into *Video/Audio*, ensure the *Video/Audio* category is monitored.



5. Click *View Application Signatures* and hover over YouTube cloud applications to view detailed information about YouTube application sensors.

Application Signature	Description	Application ID
<i>YouTube_Video.Access</i>	An attempt to access a video on YouTube.	16420
<i>YouTube_Video.Play</i>	An attempt to download and play a video from YouTube.	38569
<i>YouTube_Video.Upload</i>	An attempt to upload a video to YouTube.	22564
<i>YouTube</i>	An attempt to access YouTube. This application sensor does not depend on SSL deep inspection so it does not have a cloud or lock icon.	31077
<i>YouTube_Channel.Access</i>	An attempt to access a video on a specific channel on YouTube.	41598
<i>YouTube_Channel.ID</i>	An attempt to access a video on a specific channel on YouTube.	44956
<i>YouTube_Comment.Posting</i>	An attempt to post comments on YouTube.	31076

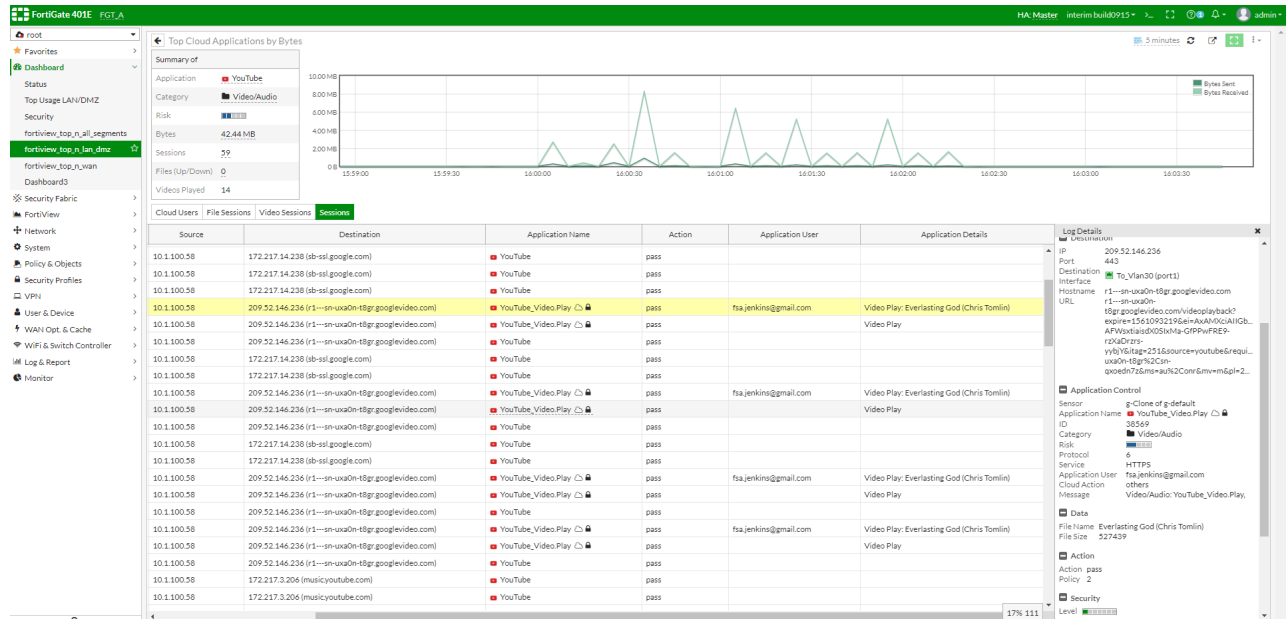
6. On the test PC, log into YouTube and play some videos.
7. On the FortiGate, go to *Log & Report > Application Control* and look for log entries for browsing and playing YouTube videos.

In this example, note the *Application User* and *Application Details*. Also note that the *Application Control ID* is 38569 showing that this entry was triggered by the application sensor *YouTube_Video.Play*.

Date/Time	%	Source	Destination	Application Name	Action	Application User	Application Details
2019/06/20 16:02:23		10.1.100.58	172.217.14.238 (sb-sst.google.com)	YouTube	pass		
2019/06/20 16:02:23		10.1.100.58	172.217.14.238 (sb-sst.google.com)	YouTube	pass		
2019/06/20 16:02:14		10.1.100.58	172.217.14.238 (sb-sst.google.com)	YouTube	pass		
2019/06/20 16:02:14		10.1.100.58	172.217.14.238 (sb-sst.google.com)	YouTube	pass		
2019/06/20 16:02:12		10.1.100.58	209.52.146.236 (r1--sn-ua0n-t8gr.googlevideo.com)	YouTube_Video.Play	pass	fsa.jenkins@gmail.com	Video Play: Everlasting God (Chris Tomlin)
2019/06/20 16:02:12		10.1.100.58	209.52.146.236 (r1--sn-ua0n-t8gr.googlevideo.com)	YouTube_Video.Play	pass		Video Play
2019/06/20 16:02:12		10.1.100.58	209.52.146.236 (r1--sn-ua0n-t8gr.googlevideo.com)	YouTube	pass		
2019/06/20 16:01:56		10.1.100.58	172.217.14.238 (sb-sst.google.com)	YouTube	pass		
2019/06/20 16:01:56		10.1.100.58	172.217.14.238 (sb-sst.google.com)	YouTube	pass		
2019/06/20 16:01:54		10.1.100.58	209.52.146.236 (r1--sn-ua0n-t8gr.googlevideo.com)	YouTube_Video.Play	pass	fsa.jenkins@gmail.com	Video Play: Everlasting God (Chris Tomlin)
2019/06/20 16:01:54		10.1.100.58	209.52.146.236 (r1--sn-ua0n-t8gr.googlevideo.com)	YouTube_Video.Play	pass		Video Play
2019/06/20 16:01:54		10.1.100.58	209.52.146.236 (r1--sn-ua0n-t8gr.googlevideo.com)	YouTube	pass		
2019/06/20 16:01:50		10.1.100.58	172.217.14.238 (sb-sst.google.com)	YouTube	pass		
2019/06/20 16:01:50		10.1.100.58	172.217.14.238 (sb-sst.google.com)	YouTube	pass		
2019/06/20 16:01:48		10.1.100.58	209.52.146.236 (r1--sn-ua0n-t8gr.googlevideo.com)	YouTube_Video.Play	pass	fsa.jenkins@gmail.com	Video Play: Everlasting God (Chris Tomlin)
2019/06/20 16:01:48		10.1.100.58	209.52.146.236 (r1--sn-ua0n-t8gr.googlevideo.com)	YouTube_Video.Play	pass		Video Play
2019/06/20 16:01:39		10.1.100.58	209.52.146.236 (r1--sn-ua0n-t8gr.googlevideo.com)	YouTube	pass		
2019/06/20 16:01:39		10.1.100.58	209.52.146.236 (r1--sn-ua0n-t8gr.googlevideo.com)	YouTube_Video.Play	pass	fsa.jenkins@gmail.com	Video Play: Everlasting God (Chris Tomlin)
2019/06/20 16:01:39		10.1.100.58	209.52.146.236 (r1--sn-ua0n-t8gr.googlevideo.com)	YouTube_Video.Play	pass		Video Play
2019/06/20 16:01:39		10.1.100.58	209.52.146.236 (r1--sn-ua0n-t8gr.googlevideo.com)	YouTube	pass		
2019/06/20 16:01:34		10.1.100.58	172.217.3.206 (music.youtube.com)	YouTube	pass		
2019/06/20 16:01:34		10.1.100.58	172.217.3.206 (music.youtube.com)	YouTube	pass		
2019/06/20 16:01:34		10.1.100.58	172.217.3.206 (music.youtube.com)	HTTPS BROWSER	pass		
2019/06/20 16:01:26		10.1.100.58	162.125.1.1 (www.dropbox.com)	Dropbox	pass		
2019/06/20 16:01:26		10.1.100.58	172.217.3.206 (music.youtube.com)	YouTube	pass		
2019/06/20 16:01:26		10.1.100.58	172.217.3.206 (music.youtube.com)	YouTube	pass		
2019/06/20 16:01:26		10.1.100.58	172.217.3.206 (music.youtube.com)	YouTube	pass		
2019/06/20 16:01:26		10.1.100.58	172.217.3.206 (music.youtube.com)	HTTPS BROWSER	pass		
2019/06/20 16:01:26		10.1.100.58	172.217.3.206 (music.youtube.com)	HTTPS BROWSER	pass		
2019/06/20 16:01:25		10.1.100.90	208.91.114.149 (chbs2.fortiguard.com)	SSL_SSLV3	pass		SSLv3
2019/06/20 16:01:25		10.1.100.90	208.91.114.149 (chbs2.fortiguard.com)	SSL	pass		
2019/06/20 16:01:25		10.1.100.90	208.91.114.149 (chbs2.fortiguard.com)	HTTPS BROWSER	pass		
2019/06/20 16:01:23		10.1.100.58	209.52.146.236 (r1--sn-ua0n-t8gr.googlevideo.com)	YouTube_Video.Play	pass	fsa.jenkins@gmail.com	Video Play: Everlasting God (Chris Tomlin)
2019/06/20 16:01:23		10.1.100.58	209.52.146.236 (r1--sn-ua0n-t8gr.googlevideo.com)	YouTube_Video.Play	pass		Video Play
2019/06/20 16:01:23		10.1.100.58	209.52.146.236 (r1--sn-ua0n-t8gr.googlevideo.com)	YouTube	pass		

8. Go to *Dashboard > Top Usage LAN/DMZ*.
9. In the *Top Cloud Application by Bytes* widget, double-click *YouTube* to drill down to view details.

10. Select the *Sessions* tab to see all the entries for the videos played. Check the sessions for *YouTube_Video.Play* with the ID 38569.



Example of monitoring network traffic without SSL deep inspection

This is an example of monitoring network traffic for YouTube via FortiView cloud application view without SSL deep inspection.

To monitor network traffic without SSL deep inspection:

1. Use a firewall policy with the following settings. If necessary, create a policy with these settings.
 - *Application Control* is enabled.
 - *SSL Inspection* is set to *certificate-inspection*.

- *Log Allowed Traffic* is set to *All Sessions*.

Inspection Mode **Flow-based** Proxy-based

Firewall / Network Options

NAT ☒

IP Pool Configuration **Use Outgoing Interface Address** Use Dynamic IP Pool

Preserve Source Port ☐

Protocol Options **PRX** default

Security Profiles

AntiVirus ☐

Web Filter ☐

DNS Filter ☐

Application Control ☒ **APP** g-Clone of g-default

IPS ☒ **IPS** g-Clone of g-default

VoIP ☐

SSL Inspection **SSL** certificate-inspection

Mirror SSL Traffic to Interfaces ☐

Logging Options

Log Allowed Traffic ☒ Security Events **All Sessions**

Capture Packets ☐

Comments 0/1023

Enable this policy ☒

2. On the test PC, log into YouTube and play some videos.
3. On the FortiGate, go to *Log & Report > Application Control* and look for log entries for browsing and playing YouTube videos.

In this example, the log shows only applications with the name YouTube. The log cannot show YouTube application sensors which rely on SSL deep inspection.

FortiGate 401E FGT-1A
HA Master interim build#912
admin

root

★ Favorites

Dashboard

✕ Security Fabric

View/FortView

+ Network

System

Policy & Objects

Security Profiles

VPN

User & Device

WAN Opt. & Cache

WiFi & Switch Controller

Log & Report

Forward Traffic

Local Traffic

Multicast Traffic

Sniffer Traffic

Events

AntiVirus

Web Filter

DNS Query

Web Application Firewall

Application Control

Intrusion Prevention

Anomaly

Anti-Spam

Data Leak Prevention

VoIP

FortiGate Cloud Reports

Log Settings

Threat Weight

Email Alert Settings

Monitor

🔄

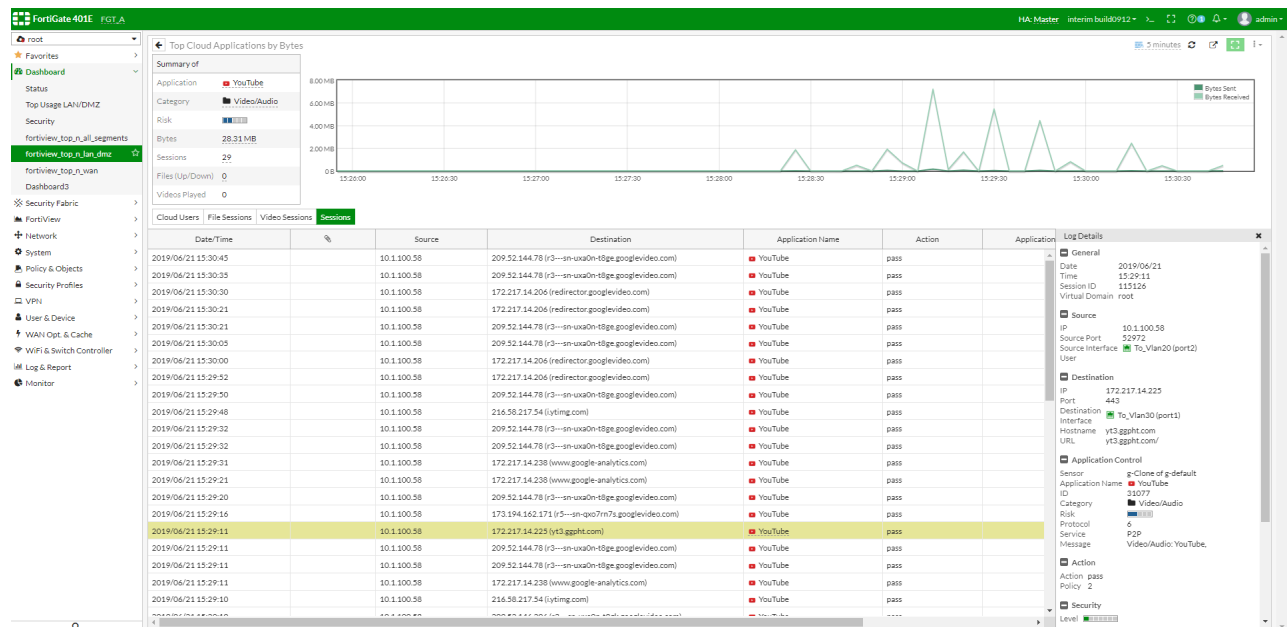
📁

🔍 Add Filter

Date/Time	Source	Destination	Application Name	Action	Application User	Application Details
2019/06/21 15:29:11	10.1.100.58	172.217.14.225 (yt3.ggpht.com)	YouTube	pass		
2019/06/21 15:29:11	10.1.100.58	172.217.14.238 (www.google-analytics.com)	QUIC	block		
2019/06/21 15:29:11	10.1.100.58	209.52.144.78 (r3---sn-uxa0n-t8jg.googlevideo.com)	YouTube	pass		
2019/06/21 15:29:11	10.1.100.58	209.52.144.78 (r3---sn-uxa0n-t8jg.googlevideo.com)	YouTube	pass		
2019/06/21 15:29:11	10.1.100.58	172.217.14.238 (www.google-analytics.com)	YouTube	pass		
2019/06/21 15:29:10	10.1.100.58	216.58.217.54 (lytimg.com)	YouTube	pass		
2019/06/21 15:29:10	10.1.100.58	216.58.217.54 (lytimg.com)	HTTPS.BROWSER	pass		
2019/06/21 15:29:10	10.1.100.58	172.217.14.194 (adservice.google.com)	Google Ads	pass		
2019/06/21 15:29:10	10.1.100.58	209.52.146.206 (r3---sn-uxa0n-t8jg.googlevideo.com)	YouTube	pass		
2019/06/21 15:29:10	10.1.100.58	209.52.146.206 (r3---sn-uxa0n-t8jg.googlevideo.com)	YouTube	pass		
2019/06/21 15:29:10	10.1.100.58	209.52.146.44 (r1---sn-uxa0n-t8jg.googlevideo.com)	YouTube	pass		
2019/06/21 15:29:10	10.1.100.58	209.52.146.44 (r1---sn-uxa0n-t8jg.googlevideo.com)	YouTube	pass		
2019/06/21 15:29:10	10.1.100.58	209.52.146.44 (r1---sn-uxa0n-t8jg.googlevideo.com)	YouTube	pass		
2019/06/21 15:29:10	10.1.100.58	209.52.146.44 (r1---sn-uxa0n-t8jg.googlevideo.com)	YouTube	pass		
2019/06/21 15:29:09	10.1.100.58	172.217.14.194 (adservice.google.com)	QUIC	block		
2019/06/21 15:29:05	10.1.100.58	209.52.146.142 (r3---sn-uxa0n-t8jg.googlevideo.com)	YouTube	pass		
2019/06/21 15:29:05	10.1.100.58	209.52.146.142 (r3---sn-uxa0n-t8jg.googlevideo.com)	YouTube	pass		
2019/06/21 15:29:05	10.1.100.58	209.52.146.142 (r3---sn-uxa0n-t8jg.googlevideo.com)	YouTube	pass		
2019/06/21 15:29:05	10.1.100.58	216.58.193.65 (tpc.googleusercontent.com)	QUIC	block		
2019/06/21 15:29:05	10.1.100.58	172.217.14.225 (yt3.ggpht.com)	YouTube	pass		
2019/06/21 15:29:05	10.1.100.58	209.52.146.142 (r3---sn-uxa0n-t8jg.googlevideo.com)	QUIC	block		
2019/06/21 15:29:05	10.1.100.58	172.217.14.194 (adservice.google.com)	QUIC	block		
2019/06/21 15:29:05	10.1.100.58	216.58.193.65 (tpc.googleusercontent.com)	Google Ads	pass		
2019/06/21 15:29:05	10.1.100.58	209.52.146.16 (r5---sn-uxa0n-t8jg.googlevideo.com)	YouTube	pass		
2019/06/21 15:29:05	10.1.100.58	172.217.14.206 (redirector.googlevideo.com)	YouTube	pass		
2019/06/21 15:29:05	10.1.100.58	172.217.14.206 (redirector.googlevideo.com)	HTTPS.BROWSER	pass		
2019/06/21 15:29:04	10.1.100.58	209.52.146.16 (r5---sn-uxa0n-t8jg.googlevideo.com)	YouTube	pass		
2019/06/21 15:29:04	10.1.100.58	172.217.14.206 (redirector.googlevideo.com)	YouTube	pass		
2019/06/21 15:29:04	10.1.100.58	172.217.14.206 (redirector.googlevideo.com)	HTTPS.BROWSER	pass		
2019/06/21 15:29:04	10.1.100.58	209.52.146.236 (r1---sn-uxa0n-t8jg.googlevideo.com)	YouTube	pass		
2019/06/21 15:29:04	10.1.100.58	172.217.3.206 (sytimg.com)	QUIC	block		
2019/06/21 15:29:00	10.1.100.58	172.217.14.194 (adservice.google.com)	Google Ads	pass		
2019/06/21 15:28:46	10.1.100.58	172.217.14.238 (www.google-analytics.com)	YouTube	pass		

General

4. Go to *Dashboard > Top Usage LAN/DMZ* and check the *Top Cloud Application by Bytes* widget. The *Top Cloud Application by Bytes* widget shows the YouTube cloud application without the video played information that requires SSL deep inspection.
5. Double-click *YouTube* and select the *Sessions* tab. These sessions were triggered by the application sensor *YouTube* with the ID *31077*. This is the application sensor with cloud behavior which does not rely on SSL deep inspection.



FortiView Sources usability

The *Sources* view displays avatar and device information (for real-time and historical views). You can also create or edit device or address definitions.

To view avatar and device information:

1. Go to *FortiView > Sources*. A list of sources displays.

Source	Device	Bytes	Sessions	Bandwidth
172.18.62.3				
172.18.64.126	00:09:0f:da:1fad	101.29 MB	48	27.34 kbps
fhou 172.18.62.40 frank.hou33@hotmail.com FENG HOU	VAN-200492-PC	82.06 MB	32	5.50 kbps
njoshi 172.18.62.243	VAN-MIS-NB1	55.25 MB	26	219.91 kbps
172.18.62.121	90:6c:acd3:f6:c6	53.84 MB	91	4.20 kbps
10.6.30.149	00:0c:29:c4:3b:26	48.94 MB	11	2.88 kbps

2. Right-click on a source and select *Drill Down to Details*. The *Summary of* box displays the avatar and device details.

Destination	Application	Bytes	Sessions	Bandwidth
oak.fortinet.com (172.16.100.80)	TCP/445	74.40 MB	1	80 bps
13.107.42.11	Microsoft.Outlook	3.19 MB	1	8.39 kbps
v20.events.data.microsoft.com (52.114.132.73)	Microsoft.Office365.Published	1.18 MB	1	1.16 kbps
sn2-client-s.gateway.messenger.live.com (52.171.217.9)	Microsoft.Azure	760.23 kB	1	544 bps
mail.fortinet-us.com (208.91.113.36)	Fortinet.FortiCloud	593.54 kB	4	112 bps
192.168.100.185	TCP/8888 UDP/60794	551.81 kB	3	56 bps
clienttwins.windows.com (13.89.220.65)	Microsoft.Azure	400.33 kB	1	32 bps
203.205.147.167	TCP/80	263.71 kB	1	104 bps
CA-VAN-ANK-R006.teamviewer.com (188.172.213.73)	TeamViewer.TeamViewer	162.63 kB	1	40 bps
40.122.76.193	Microsoft.Azure	126.83 kB	1	40 bps

To create or edit definitions in the top level view:

1. Go to *FortiView > Sources*.
2. Right-click on a source.

3. Select an option. In this example, *Create Custom Device* is selected.

Source	Device	Bytes	Sessions	Bandwidth
172.18.64.180		12.36 MB	43	1.95 kbps
172.18.64.129	90:6ciac:90:9ba0	11.95 MB	11	728 bps
172.18.62.40	VAN-200492-PC	11.14 MB	36	21.94 kbps
172.18.62.61	DESKTOP-036J80V	10.92 MB	42	1.17 kbps
172.18.64.126	00:09:0f:da:1f:ad	10.71 MB	44	8.65 kbps

To create or edit definitions in the drill down view:

1. In the *Summary of* box, click the *Actions* button.
2. Select an option. In this example, *Edit Custom Device* is selected.

Destination	Application	Bytes	Sessions	Bandwidth
129.213.48.93	Oracle:OracleCloud	26.89 MB	1	0 bps
173.243.138.221	Fortinet:FortiGuard	1.81 MB	1	0 bps
62.209.40.75	Fortinet:FortiGuard	1.81 MB	1	0 bps
208.91.112.220	Fortinet:FortiGuard	1.81 MB	1	0 bps
45.75.200.89	Fortinet:FortiGuard	1.80 MB	1	0 bps
209.222.147.38	Fortinet:FortiGuard	1.80 MB	1	0 bps
service.fortiguards.net (192.168.100.206)	UDP/8888	1.40 MB	3	0 bps
10.10.10.255	UDP/8014	610.14 KB	1	0 bps

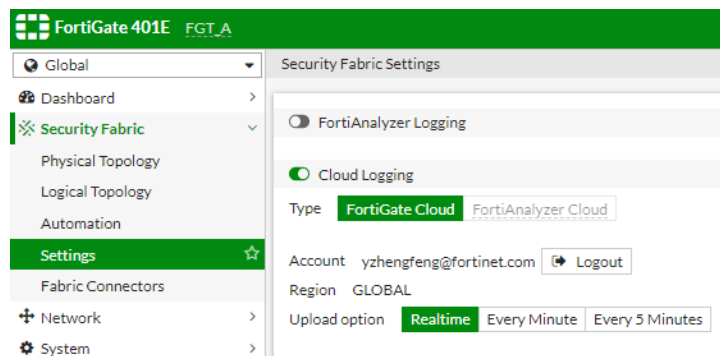
FortiView from FortiGate Cloud

This function requires a FortiGate that is registered and logged into a compatible FortiGate Cloud.

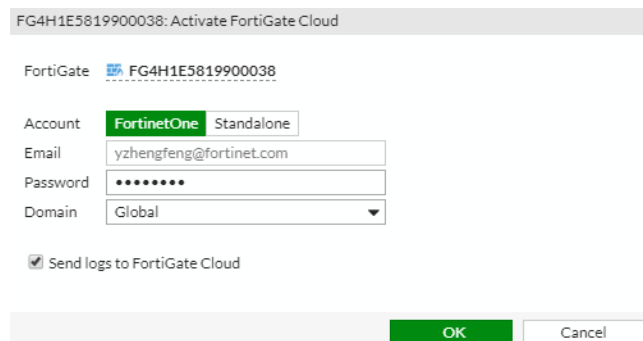
To enable FortiView with log source as FortiGate Cloud:

1. Go to *Security Fabric > Settings*.
2. Enable *Cloud Logging* and select *FortiGate Cloud*.

If the FortiGate is registered and logged into FortiGate Cloud, the *Account* and *Region* is displayed.



If the FortiGate is logged out from FortiGate Cloud, click *Activate* and log in, and ensure *Send logs to FortiGate Cloud* is selected.



3. Go to *Log & Report > Log Settings* and set the following:

- Set *Event Logging* to *All*.
- Set *Local Traffic Log* to *All*.

FortiGate 401E FGT_A

Log Settings

Send logs to syslog ☐

Cloud Logging

Type **FortiGate Cloud** FortiAnalyzer Cloud

Account yzhengfeng@fortinet.com Logout

Region GLOBAL

Upload option **Realtime** Every Minute Every 5 Minutes

Logs Sent to FortiGate Cloud Daily

70.00 MB
60.00 MB
50.00 MB
40.00 MB
30.00 MB
20.00 MB
10.00 MB
0 B

Jun 12 Jun 13 Jun 14 Jun 15 Jun 16 Jun 17 Jun 18

Traffic Log Event Log AntiVirus Log Web Filter Log IPS Log DLP log Application Control Log WAF Log
DNS Query Log log_type_ssl

Log Settings

Event Logging **All** Customize

Local Traffic Log **All** Customize

GUI Preferences

Resolve Hostnames ☒

Resolve Unknown Applications ☒

Apply

4. Go to *FortiView > Sources*.

The top right has a dropdown menu to select the source.

FortiGate 401E FGT_A

HA: Master interim build09222

admin

Source Device Threat Score Bytes Sessions Source

10.1.100.90	WIN764B90	0	89.61 MB	2,921	10.1.100.90
10.1.100.58	W7OUTLOOKC	0	5.42 MB	1,621	10.1.100.58
2000:10:1:100:0:0:0:90	WIN764B90	0	448.80 KB	22	2000:10:1:100:0:0:0:90

Source: FortiGates, FortiAnalyzer, FortiGate Cloud

5. In the top right dropdown menu, select *FortiGate Cloud* as the source.

Source	Device	Threat Score	Bytes	Sessions	Source Interface
10.1.100.90 High Risk	WIN764B90	0	89.61 MB	2,921	To_Vlan20 (port12)
10.1.100.58 Medium Risk	W70UTLOOKC	0	5.42 MB	1,621	To_Vlan20 (port12)
2000:10:1:100:0:0:0:90 High Risk	WIN764B90	0	448.80 kB	22	To_Vlan20 (port12)
10.1.100.11	00:0c:29:9f:03:a7	0	3.92 kB	9	To_Vlan20 (port12)

You can select FortiGate Cloud as the data source for all available FortiView pages and widgets.

Supported views for different log sources

The following chart identifies what log sources support which views:

	Disk for FortiOS 6.2.0	FortiAnalyzer 6.2.0	FortiGate Cloud 4.1.1
Sources	Yes	Yes	Yes
Admin logins	Yes	Yes	No
Applications	Yes	Yes	Yes
Cloud Applications	No	No	No
Cloud User	Yes	Yes	No
Destination Countries MAP	Yes	Yes	Yes
Destination Countries Table View	Yes	Yes	Yes
Destination Countries Bubble View	Yes	Yes	Yes
Destination Interface	Yes	Yes	Yes
Destination IPS	Yes	Yes	Yes
Destination Owners	Yes	Yes	No
Destination Firewall Objects	Yes	Yes	No
Endpoint Devices	Yes	Yes	Yes
Endpoint Vulnerability	Yes	Yes	No
Failed Authentication	Yes	Yes	Yes
Interface Pair	Yes	Yes	No
Policies	Yes	Yes	Yes

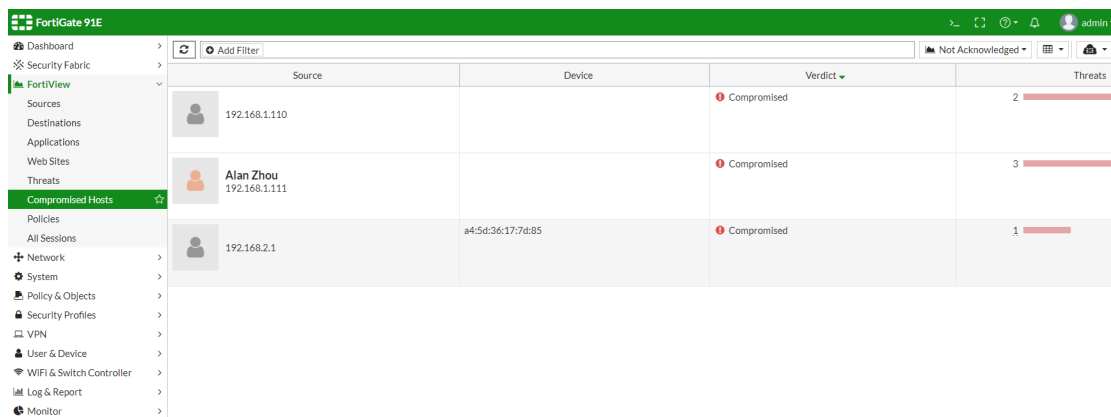
	Disk for FortiOS 6.2.0	FortiAnalyzer 6.2.0	FortiGate Cloud 4.1.1
Search Phrases	Yes	Yes	No
Source Interface	Yes	Yes	Yes
Source Firewall Objects	Yes	Yes	No
System Events	Yes	Yes	Yes
Threats	Yes	Yes	Yes
Top FortiSandbox Files by Submitted	Yes	Yes	No
VPN	Yes	Yes	Yes
Web Category	Yes	Yes	Yes
Web Sites	Yes	Yes	Yes
WiFi Clients	Yes	Yes	No

FortiGate Cloud-based IOC

Topology, FortiView, and automation support Indicators of Compromise (IOC) detection from the FortiGate Cloud IOC service.

FortiGate lists IOC entries on the *FortiView* pane, and uses the IOC event logs as a trigger for automation stitches. IOC and web filter licenses are required to use this feature. You must also enable FortiGate Cloud logging on the FortiGate.

To view compromised hosts, go to *FortiView > Compromised Hosts*. The IOC entries are displayed when the source is FortiGate Cloud.



Source	Device	Verdict	Threats
192.168.1.110		Compromised	2
Alan Zhou 192.168.1.111		Compromised	3
192.168.2.1	a4:5d:36:17:7d:85	Compromised	1

You can also view the IOC entries in the FortiGate Cloud portal.

FortiView — subnet filters

In FortiView, you can filter source IPs or destination IPs with a subnet mask using the x.x.x.x/x format. You can view the results in real-time or historical mode.



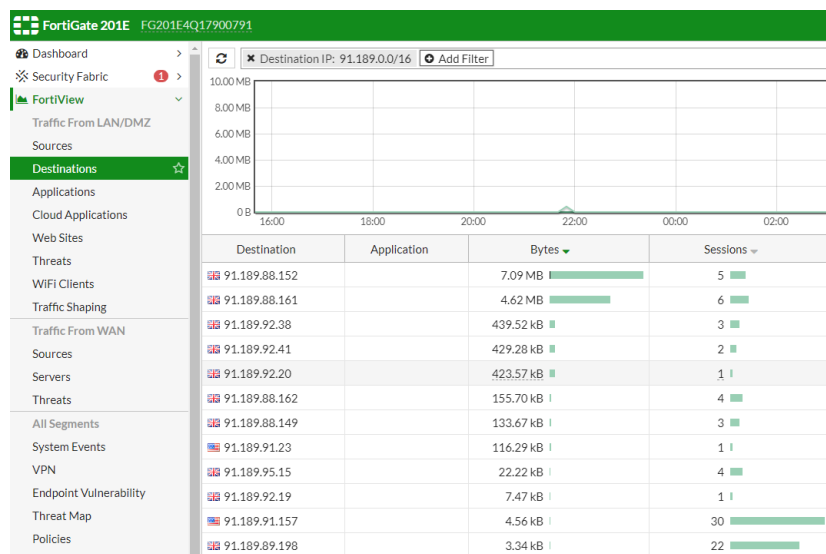
Both logging from disk and logging from FortiAnalyzer are supported.

Sample configuration of filtering IPs with a subnet mask

This example shows how to filter destination IPs with a subnet mask using the x.x.x.x/x format.

To filter destination IPs with a subnet mask:

1. Go to *FortiView* > *Destinations*.
2. Click *Add Filter*.
3. In the dropdown menu, select *Destination IP*.
4. Enter the subnet mask (in the example, *91.189.0.0/16*).
5. Press the **Enter** key. The filter results display.



To view results in the backend subnet filter:

```
# diagnose device application miglogd 0x70000
Debug messages will be on for unlimited time.
```

```
# fortiview_add_filter_field_ex()-1559: fortiview add filter field:"destination"=>"dstip"
```

```

type:4 negate:0
fortiview_add_filter_field_ex()-1560: values:
fortiview_add_filter_field_ex()-1562: value[0]=91.189.0.0/16
fortiview_add_filter_field_ex()-1559: fortiview add filter
field:"srcintfrole"=>"srcintfrole" type:4 negate:0
fortiview_add_filter_field_ex()-1560: values:
fortiview_add_filter_field_ex()-1562: value[0]=lan
fortiview_add_filter_field_ex()-1562: value[1]=dmz
fortiview_add_filter_field_ex()-1562: value[2]=undefined
__params_from_filter()-583: filter field:dstip 91.189.0.0/16
__params_from_filter()-583: filter field:srcintfrole lan
__params_from_filter()-583: filter field:srcintfrole dmz
__params_from_filter()-583: filter field:srcintfrole undefined
fortiview_request_data()-896: dataset:fv.dest.group tabid:0
_dump_sql()-829: dataset=fv.dest.group, sql:select dstip, max(dstintf) dst_intf,max
(dstdevtype) dst_devtype,max(dstmac) dst_mac,group_concat(distinct appid) appid,group_concat
(distinct appservice||case when subapp is null then '' else '_'||subapp end) appname,sum
(sessioncount) session_count, sum(case when passthrough<>'block' then sessioncount else 0
end) session_allow, sum(case when passthrough='block' then sessioncount else 0 end) session_
block, sum(rcvdbyte) r, sum(sentbyte) s, sum(rcvdbyte + sentbyte) bandwidth ,sum(crscore)
score, sum(case when passthrough<>'block' then crscore else 0 end) score_allow, sum(case
when passthrough='block' then crscore else 0 end) score_block from grp_traffic_all_dst
where timestamp between 1551397800 and 1551484200 and l=1 AND ( ft_ipmask(dstip, 0,
'91.189.0.0/16') ) AND srcintfrole in ('lan','dmz','undefined') group by dstip order by
bandwidth desc limit 100;
takes 10(ms), agggr:0(ms)

fortiview_request_data()-933: total:12 start:1551397800 end:1551484200
__params_from_filter()-583: filter field:dstip 91.189.0.0/16
__params_from_filter()-583: filter field:srcintfrole lan
__params_from_filter()-583: filter field:srcintfrole dmz
__params_from_filter()-583: filter field:srcintfrole undefined
fortiview_request_data()-896: dataset:fv.general.chart tabid:0
_dump_sql()-829: dataset=fv.general.chart, sql:select a.timestamp1,ses_al,ses_bk,r,s,ifnull
(sc_l,0),ifnull(sc_m,0),ifnull(sc_h,0),ifnull(sc_c,0) from (select timestamp-(timestamp%600)
timestamp1 ,sum(case when passthrough<>'block' then sessioncount else 0 end) ses_al,sum(case
when passthrough='block' then sessioncount else 0 end) ses_bk,sum(rcvdbyte) r,sum(sentbyte)
s from grp_traffic_all_dst where timestamp BETWEEN 1551397800 and 1551484199 and l=1 AND (
ft_ipmask(dstip, 0, '91.189.0.0/16') ) AND srcintfrole in ('lan','dmz','undefined') group
by timestamp1 ) a left join (select timestamp-(timestamp%600) timestamp1 ,sum(case when
threat_level=1 then crscore else 0 end) sc_l,sum(case when threat_level=2 then crscore else
0 end) sc_m,sum(case when threat_level=3 then crscore else 0 end) sc_h,sum(case when threat_
level=4 then crscore else 0 end) sc_c from grp_threat where timestamp BETWEEN 1551397800
and 1551484199 and l=1 AND ( ft_ipmask(dstip, 0, '91.189.0.0/16') ) AND srcintfrole in
('lan','dmz','undefined') group by timestamp1 ) b on a.timestamp1 = b.timestamp1;
takes 30(ms), agggr:0(ms)

fortiview_request_data()-933: total:47 start:1551397800 end:1551484199

```

FortiView dashboards and widgets

FortiView is consolidated within the System Dashboards. FortiView pages are available as widgets that can be added to the flexible dashboards.

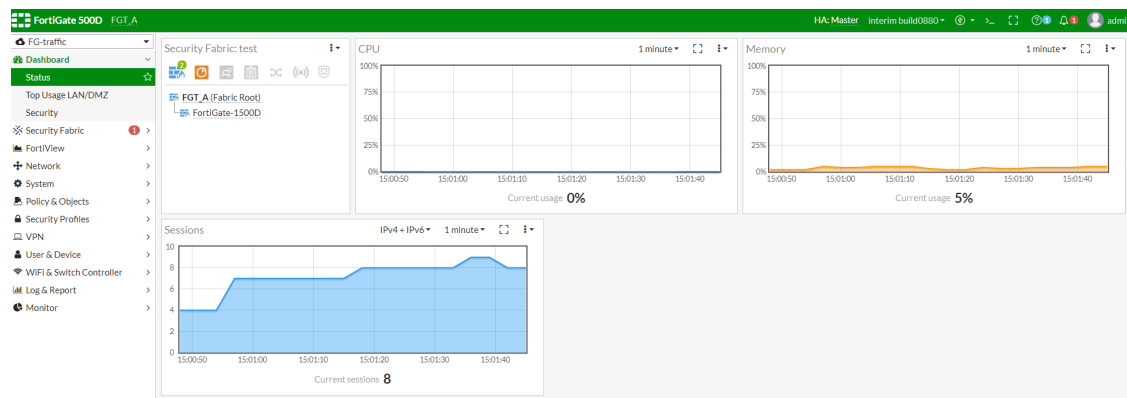


Only core FortiView pages are available in the *FortiView* menu. All non-core FortiView pages are available as dashboard widgets.

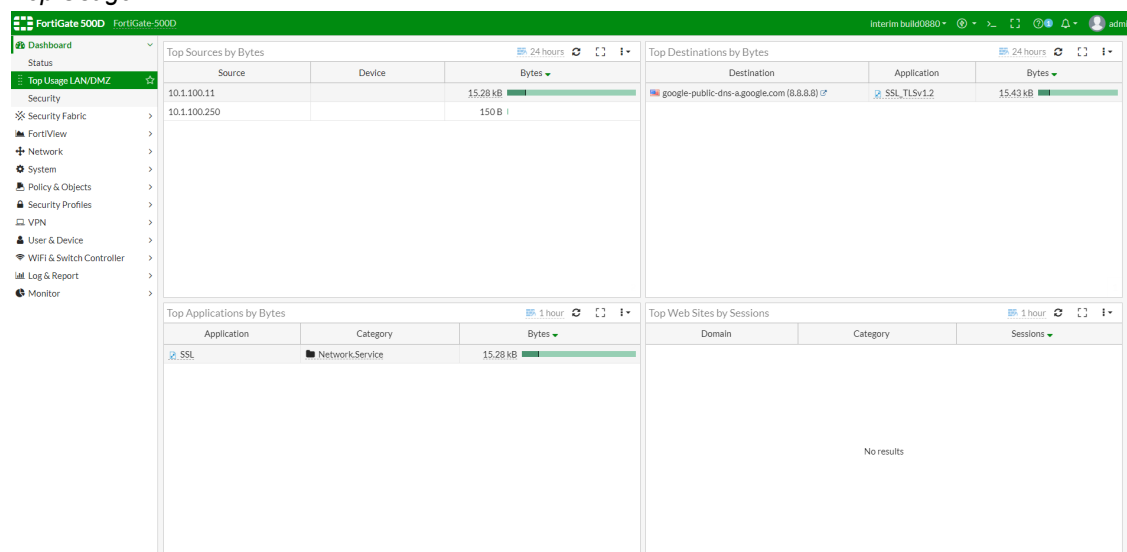
Dashboards are available per VDOM.

The *Dashboard* menu contains the following:

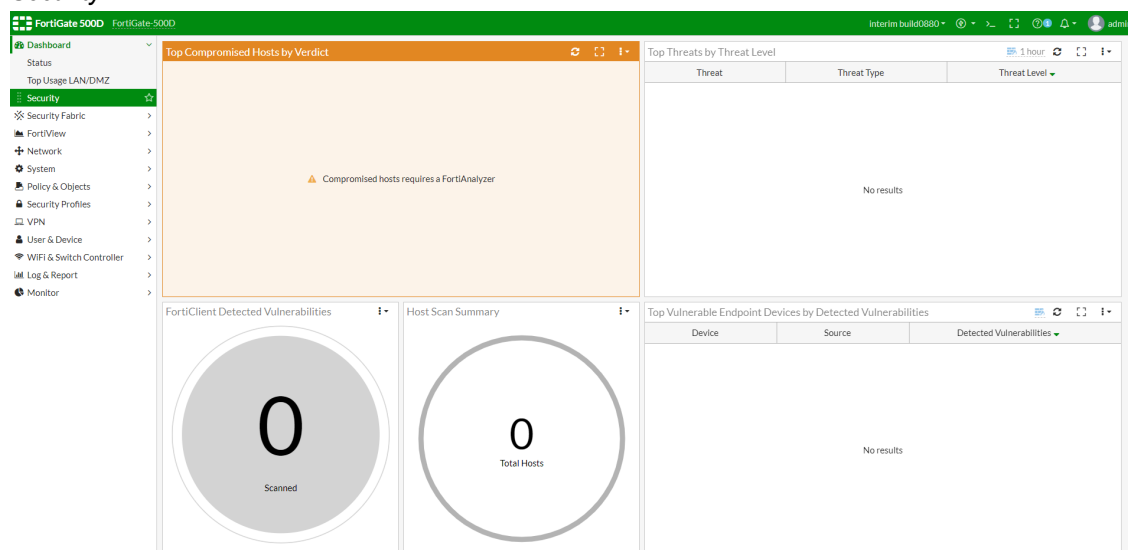
- **Status dashboard**



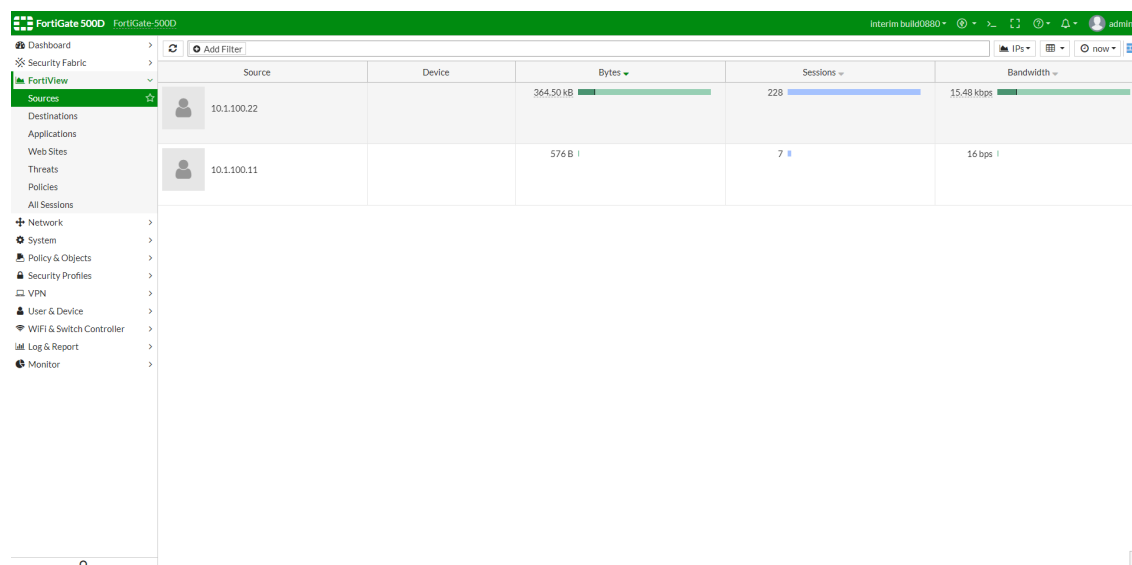
- **Top Usage LAN/DMZ dashboard**



- Securitydashboard



Only core FortiView pages are available in the *FortiView* menu.



All non-core FortiView pages are available as dashboard widgets.

To add a FortiView widget in the dashboard:

1. Within the *Dashboard* menu, select the dashboard you wish to edit (in the example, *Top Usage LAN/DMZ*).
2. Click the gear button in the bottom-right corner of the screen.
3. Click *Add Widget*.
4. Under the *FortiView* section, select *FortiView Top N*. The *Add Dashboard Widget* pane opens.
5. Under the *FortiView* dropdown, select the widget. There are three submenus to choose from: *LAN/DMZ*, *WAN*, or *All Segments*.

FortiGate 5000 FortiView

Interim build03890 - admin

Top Sources by Bytes (24 hours)

Source	Device	Bytes
10.1.100.11		19.72 kB
10.1.100.22		152 B
10.1.100.250		150 B

Top Applications by Bytes (1 hour)

Application	Category	Bytes
SSL	Network.Service	15.28 kB
Ping	Network.Service	3.36 kB
DNS	Network.Service	776 B
NTP	Network.Service	456 B

Add Dashboard Widget - FortiView Top N

Title: FortiView Top N

FortiView: LAN/DMZ | WAN | All Segments

Search: [Search]

Back

- Applications
- Cloud Applications
- Cloud Users
- Compromised Hosts
- Countries/Regions
- Destination Firewall Objects
- Destination Owners
- Destinations
- Search Phrases
- Source Firewall Objects
- Sources
- Threats
- Traffic Chunks

FortiGate 5000 FortiView

Interim build03890 - admin

Top Sources by Bytes (24 hours)

Source	Device	Bytes
10.1.100.11		19.72 kB
10.1.100.22		152 B
10.1.100.250		150 B

Top Applications by Bytes (1 hour)

Application	Category	Bytes
SSL	Network.Service	15.28 kB
Ping	Network.Service	3.36 kB
DNS	Network.Service	776 B
NTP	Network.Service	456 B

Add Dashboard Widget - FortiView Top N

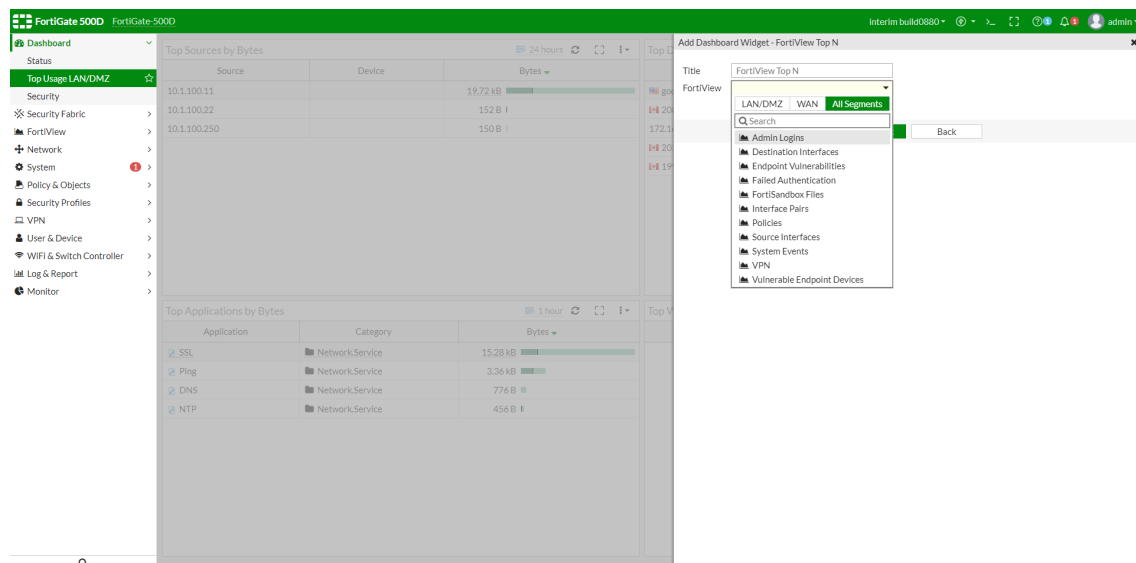
Title: FortiView Top N

FortiView: LAN/DMZ | **WAN** | All Segments

Search: [Search]

Back

- Servers
- Threats

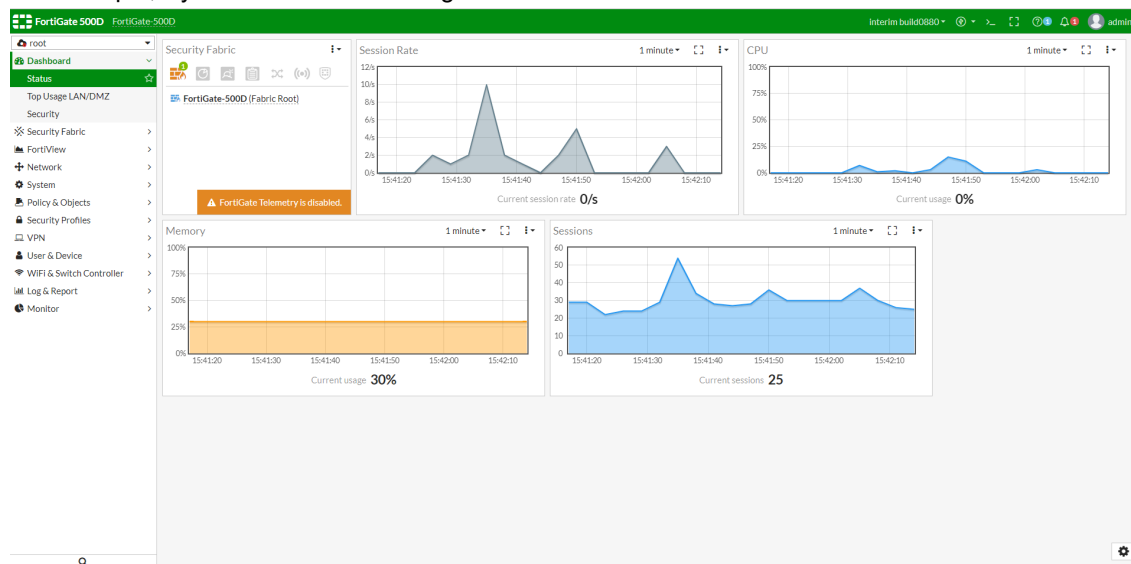


6. Configure the widget settings.
7. Click *Add Widget*.

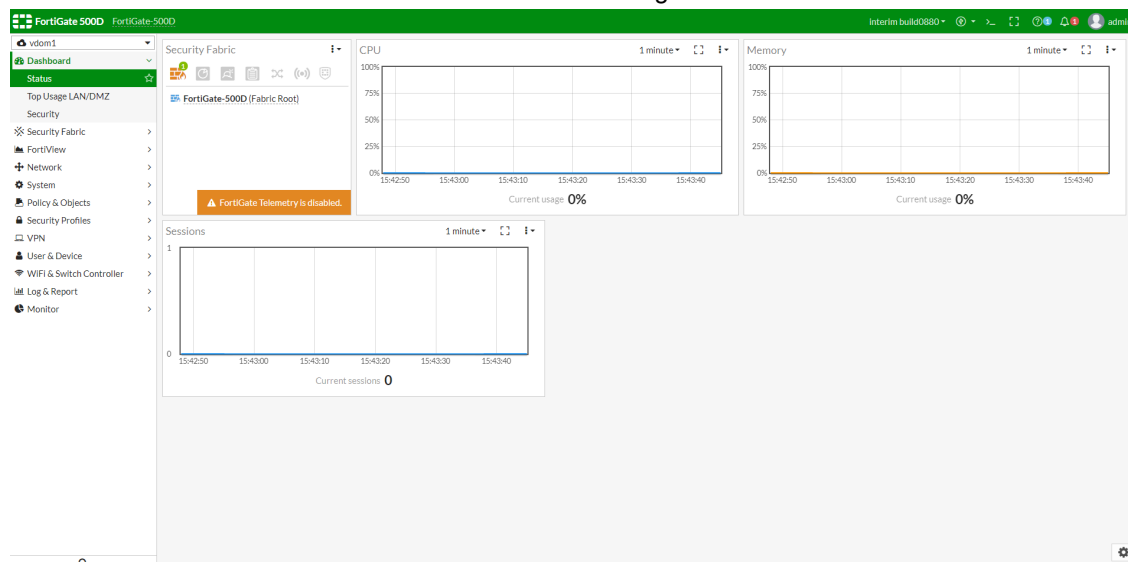
VDOMs and dashboards

Once VDOMs are enabled, dashboards are created per VDOM.

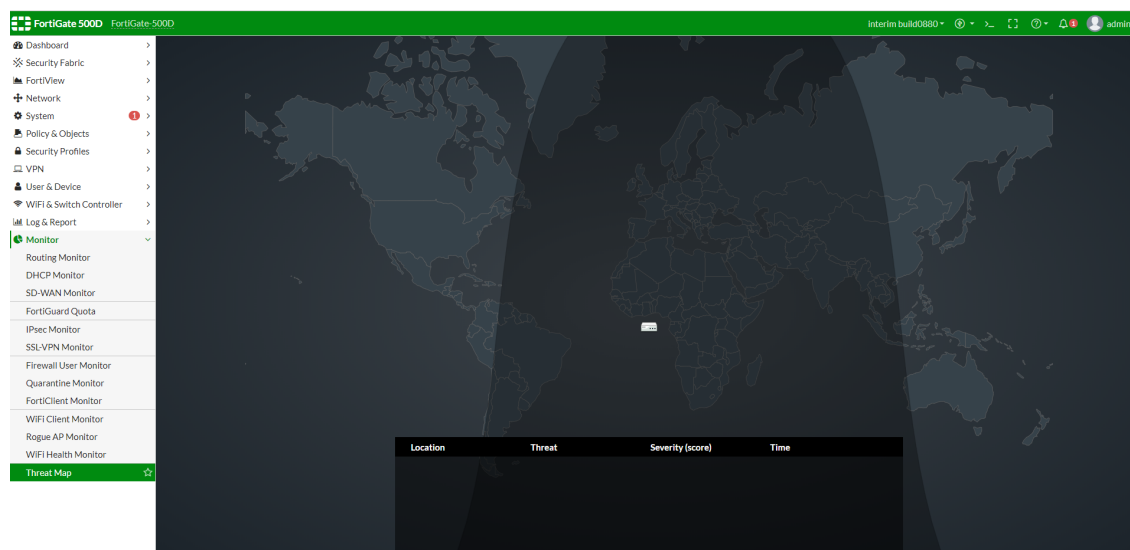
- For example, if you add a *Sessions* widget to the root VDOM as shown below:



- Notice that other VDOMs have no data in the *Sessions* widget.



The *Threat Map* is available in the *Monitor* tree menu.



FortiView object names

The FortiView *Sources* and *views leverage UUID to resolve firewall object (address) names for improved usability.*

Requirements

- The *Firewall Objects*-based view is only available when the data source is disk.
- To have a historical *Firewall Objects*-based view, address objects' UUIDs need to be logged.

To enable address object UUID logging in the CLI:

```
config system global
    set log-uuid-address enable
end
```

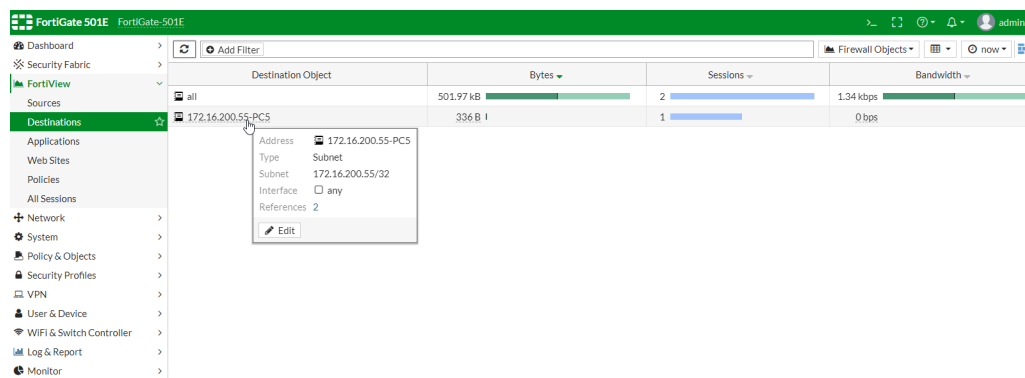
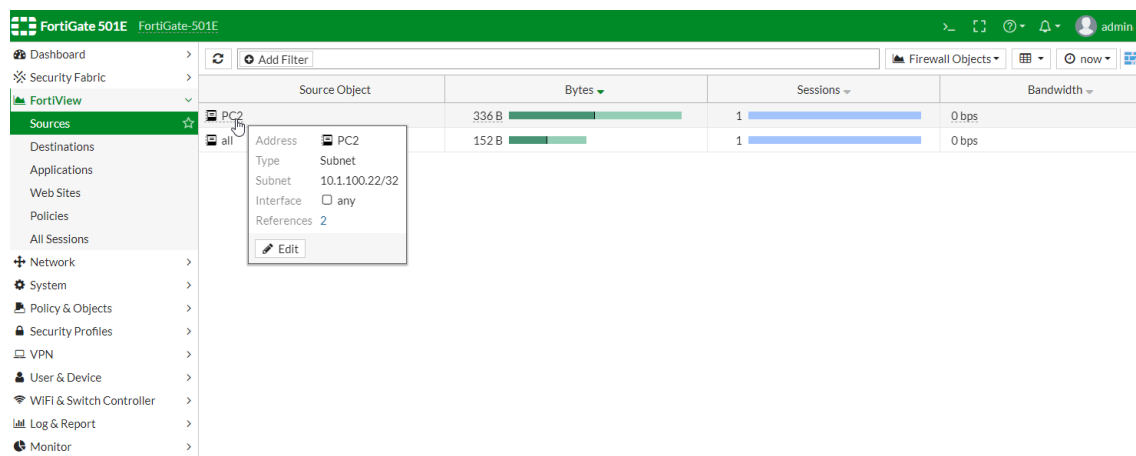
Sample configuration

In this example, firewall addresses have been configured using the commands in [To configure firewall addresses in the CLI: on page 313](#), and each firewall address object is associated with a unique UUID.

In the *Sources* and *Destinations* views, firewall objects can be displayed in real-time or in a historical chart. Objects can also be drilled down for more details.

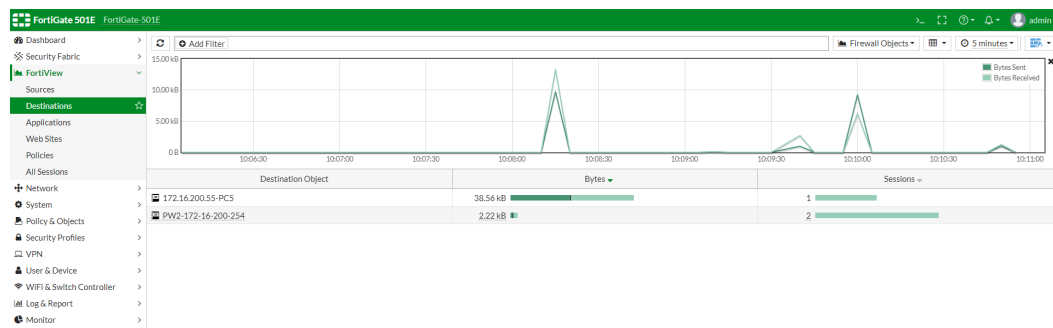
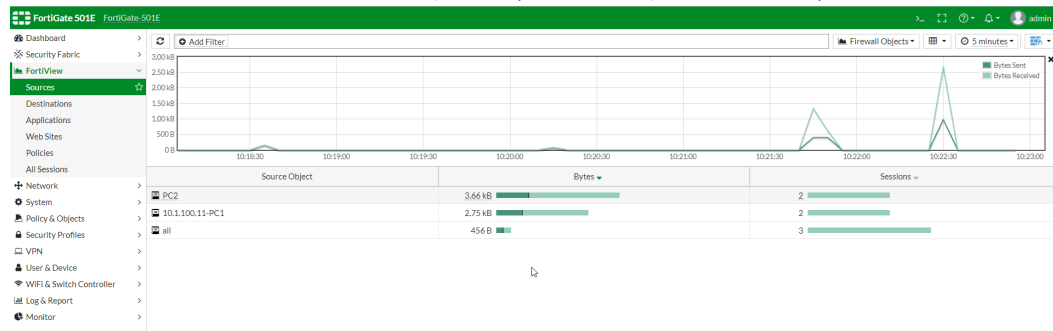
To view Firewall Object-based charts in real-time:

1. In the FortiView tree menu, select the view (*Sources* or *Destinations*).
2. In the top right corner of the settings bar:
 - a. Select *Firewall Objects* as the data criterion.
 - b. Select *now* as the time criterion.



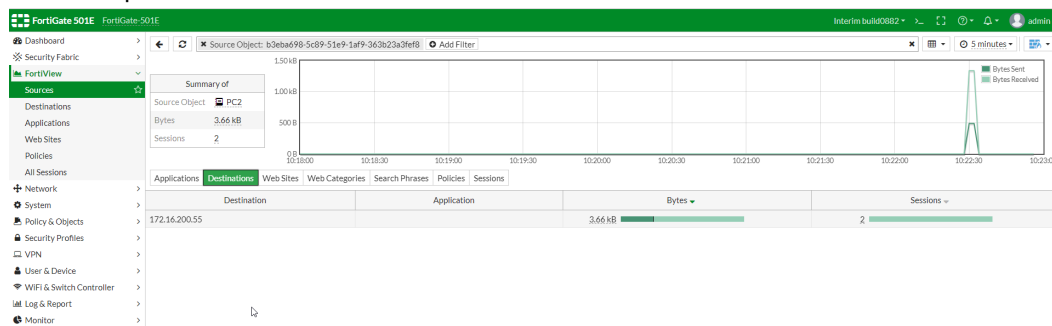
To view Firewall Object-based charts over a historical period:

1. In the FortiView menu, select the view (*Sources* or *Destinations*).
2. In the top right corner of the settings bar:
 - a. Select *Firewall Objects* as the data criterion.
 - b. Select a time criterion from the dropdown (in the examples, *5 minutes*).

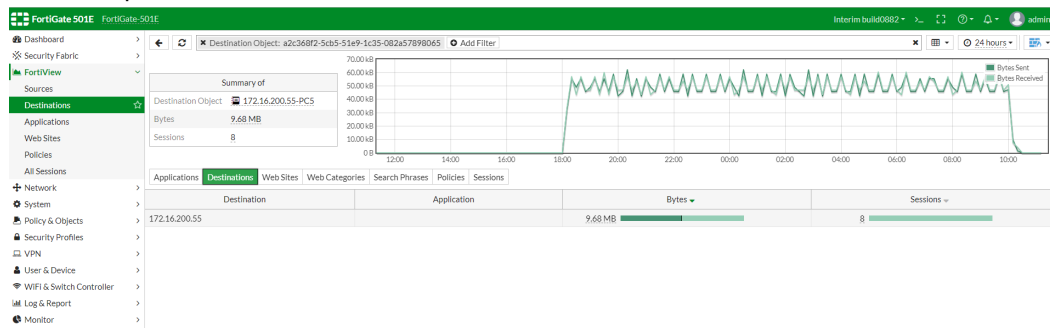


To drill down Firewall Objects:

1. Right-click on any *Source Object* or *Destination Object* in the view results.
2. Select *Drill Down to Details*. More information displays about the object; there are additional criteria to filter data.
 - This example shows a drill down of *PC2* from the *Sources* view.



- This example shows a drill down of *172.16.200.55-PC5* from the *Destinations* view.



To configure firewall addresses in the CLI:

```
config firewall address
edit "PC2"
set uuid b3eba698-5c89-51e9-1af9-363b23a3fef8
set subnet 10.1.100.22 255.255.255.255
next
edit "10.1.100.11-PC1"
set uuid 96bcba2-5cb5-51e9-bc02-465c0aab5e2c
set subnet 10.1.100.11 255.255.255.255
next
edit "172.16.200.55-PC5"
set uuid a2c368f2-5cb5-51e9-1c35-082a57898065
set subnet 172.16.200.55 255.255.255.255
next
edit "PW2-172-16-200-254"
set uuid def64b6a-5d45-51e9-5ab0-b0d0a3128098
set subnet 172.16.200.254 255.255.255.255
next
end
```

To configure the firewall policy with defined firewall addresses in the CLI:

```
config firewall policy
edit 1
set name "v4-out"
set uuid 4825ff5a-dc94-51e8-eeab-e138bc255e4a
set srcintf "port10"
set dstintf "port9"
set srcaddr "PC2" "10.1.100.11-PC1"
set dstaddr "172.16.200.55-PC5" "PW2-172-16-200-254"
set action accept
set schedule "always"
set service "ALL"
set utm-status enable
set inspection-mode proxy
set logtraffic all
set av-profile "default"
set ssl-ssh-profile "custom-deep-inspection"
set nat enable
next
edit 2
set name "to-Internet"
```

```
set uuid 28379372-5c8a-51e9-c765-cc755a07a200
set srcintf "port10"
set dstintf "port9"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set utm-status enable
set inspection-mode proxy
set logtraffic all
set av-profile "default"
set nat enable
next
end
```


Network

The following topics provide information about network settings:

- [Interfaces on page 315](#)
- [DNS on page 352](#)
- [Explicit and transparent proxies on page 363](#)
- [SD-WAN on page 451](#)
- [DHCP server on page 400](#)
- [Static routing on page 405](#)
- [Multicast on page 427](#)
- [Direct IP support for LTE/4G on page 431](#)
- [LLDP reception on page 434](#)
- [NetFlow on page 436](#)

Interfaces

Physical and virtual interfaces allow traffic to flow between internal networks, and between the internet and internal networks. FortiGate has options for setting up interfaces and groups of subnetworks that can scale as your organization grows. You can create and edit VLAN, EMAC-VLAN, switch interface, zones, and so on.

The following topics provide information about interfaces:

- [Interface settings on page 316](#)
- [Aggregation and redundancy on page 319](#)
- [VLANs on page 321](#)
- [Enhanced MAC VLANs on page 327](#)
- [Inter-VDOM routing on page 330](#)
- [Software switch on page 335](#)
- [Hardware switch on page 337](#)
- [Zone on page 338](#)
- [Virtual Wire Pair on page 340](#)
- [Virtual switch support for FortiGate 300E series on page 342](#)
- [Failure detection for aggregate and redundant interfaces on page 344](#)
- [VLAN inside VXLAN on page 344](#)
- [Virtual Wire Pair with VXLAN on page 347](#)
- [Interface MTU packet size on page 348](#)
- [One-arm sniffer on page 351](#)

Interface settings

Administrators can configure both physical and virtual FortiGate interfaces in *Network > Interfaces*. There are different options for configuring interfaces when FortiGate is in NAT mode or transparent mode.

To configure an interface in the GUI:

1. Go to *Network > Interfaces*.
2. Click *Create New > Interface*.
3. Configure the interface fields:

Interface Name	Physical interface names cannot be changed.
Alias	<p>Enter an alternate name for a physical interface on the FortiGate unit. This field appears when you edit an existing physical interface. The alias does not appear in logs.</p> <p>The maximum length of the alias is 25 characters.</p>
Type	The configuration type for the interface, such as VLAN or Software Switch.
Link Status	Indicates whether the interface is connected to a network or not (link status is up or down). This field is available when you edit an existing physical interface.
Interface	<p>This field is available when <i>Type</i> is set to <i>VLAN</i>.</p> <p>Select the name of the physical interface that you want to add a VLAN interface to. Once created, the VLAN interface is listed below its physical interface in the <i>Interface</i> list.</p> <p>You cannot change the physical interface of a VLAN interface except when you add a new VLAN interface.</p>
VLAN ID	<p>This field is available when <i>Type</i> is set to <i>VLAN</i>.</p> <p>Enter the VLAN ID. The VLAN ID can be any number between 1 and 4094 and must match the VLAN ID added by the IEEE 802.1Q-compliant router or switch that is connected to the VLAN subinterface.</p> <p>The VLAN ID cannot be edited after the interface is added.</p>
Virtual Domain	<p>Select the virtual domain to add the interface to.</p> <p>Only administrator accounts with the <i>super_admin</i> profile can change the <i>Virtual Domain</i>.</p>
Role	<p>Set the role setting for the interface. Different settings will be shown or hidden when editing an interface depending on the role.</p> <ul style="list-style-type: none"> • <i>LAN</i>: Used to connected to a local network of endpoints. It is default role for new interfaces. • <i>WAN</i>: Used to connected to the internet. When WAN is selected, the <i>Estimated bandwidth</i> setting is available, and the following settings are not: <i>DHCP server</i>, <i>Create address object matching subnet</i>, <i>Device detection</i>, <i>Security mode</i>, <i>One-arm sniffer</i>, <i>Dedicate to extension/fortiap modes</i>, and <i>Admission Control</i>.and will show Estimated Bandwidth settings. • <i>DMZ</i>: Used to connected to the DMZ. When selected, <i>DHCP server</i> and

	<p><i>Security mode</i> are not available.</p> <ul style="list-style-type: none"> • <i>Undefined</i>: The interface has no specific role. When selected, <i>Create address object matching subnet</i> is not available.
Interface Members	<p>This section can has different formats depending on the <i>Type</i>:</p> <p><i>Software Switch</i>: This field is read-only, and shows the interfaces that belong to the virtual interface of the software switch.</p> <p><i>802.3ad Aggregate or Redundant Interface</i>: This field includes the available and selected interface lists.</p>
Addressing mode	<p>Select the addressing mode for the interface.</p> <ul style="list-style-type: none"> • <i>Manual</i>: Add an IP address and netmask for the interface. If IPv6 configuration is enabled, you can add both an IPv4 and an IPv6 address. • <i>DHCP</i>: Get the interface IP address and other network settings from a DHCP server. • <i>PPPoE</i>: Get the interface IP address and other network settings from a PPPoE server. This option is only available on the low-end FortiGate models.
IP/Netmask	<p>If <i>Addressing Mode</i> is set to <i>Manual</i>, enter an IPv4 address and subnet mask for the interface. FortiGate interfaces cannot have multiple IP addresses on the same subnet.</p>
IPv6 Address/Prefix	<p>If <i>Addressing Mode</i> is set to <i>Manual</i> and IPv6 support is enabled, enter an IPv6 address and subnet mask for the interface. A single interface can have an IPv4 address, IPv6 address, or both.</p>
Create address object matching subnet	<p>This option is available when <i>Role</i> is set to <i>LAN</i> or <i>DMZ</i>.</p> <p>Enable this option to automatically create an address object that matches the interface subnet.</p>
Secondary IP Address	<p>Add additional IPv4 addresses to this interface.</p>
IPv4 Administrative Access	<p>Select the types of administrative access permitted for IPv4 connections to this interface. See Configure administrative access to interfaces on page 318.</p>
IPv6 Administrative Access	<p>Select the types of administrative access permitted for IPv6 connections to this interface. See Configure administrative access to interfaces on page 318.</p>
DHCP Server	<p>Select to enable a DHCP server for the interface.</p>
Device Detection	<p>Enable/disable passively gathering device identity information about the devices on the network that are connected to this interface.</p>
Security Mode	<p>Enable/disable captive portal authentication for this interface. After enabling captive portal authentication, you can configure the authentication portal, user and group access, custom portal messages, exempt sources and destinations/services, and redirect after captive portal.</p>
Outbound shaping profile	<p>Enable/disable traffic shaping on the interface. This allows you to enforce bandwidth limits on individual interfaces.</p>
Comments	<p>Enter a description of the interface of up to 255 characters.</p>
Status	<p>Enable/disable the interface.</p>

- **Enabled:** The interface is active and can accept network traffic.
- **Disabled:** The interface is not active and cannot accept traffic.

4. Click **OK**.

To configure an interface in the CLI:

```
config system interface
  edit "<Interface_Name>"
    set vdom "<VDOM_Name>"
    set mode static/dhcp/pppoe
    set ip <IP_address> <netmask>
    set security-mode {none | captive-portal}
    set egress-shaping-profile <Profile_name>
    set device-identification {enable | disable}
    set allowaccess ping https ssh http
    set secondary-IP enable
    config secondaryip
      edit 1
        set ip 9.1.1.2 255.255.255.0
        set allowaccess ping https ssh snmp http
      next
    end
  next
end
```

Configure administrative access to interfaces

You can configure the protocols that administrators can use to access interfaces on the FortiGate. This helps secure access to the FortiGate by restricting access to a limited number of protocols. It helps prevent users from accessing interfaces that you don't want them to access, such as public-facing ports.

As a best practice, you should configure administrative access when you're setting the IP address for a port.

To configure administrative access to interfaces in the GUI:

1. Go to *Network > Interfaces*.
2. Create or edit an interface.
3. In the *Administrative Access* section, select which protocols to enable for *IPv4* and *IPv6 Administrative Access*.

HTTPS	Allow secure HTTPS connections to the FortiGate GUI through this interface. If configured, this option is enabled automatically.
HTTP	Allow HTTP connections to the FortiGate GUI through this interface. This option can only be enabled if HTTPS is already enabled.
PING	The interface responds to pings. Use this setting to verify your installation and for testing.
FMG-Access	Allow FortiManager authorization automatically during the communication exchanges between FortiManager and FortiGate devices.
SSH	Allow SSH connections to the CLI through this interface.

SNMP	Allow a remote SNMP manager to request SNMP information by connecting to this interface.
FTM	Allow FortiToken Mobile Push (FTM) access.
RADIUS Accounting	Allow RADIUS accounting information on this interface.
Security Fabric Connection	Allow Security Fabric access. This enables FortiTelemetry and CAPWAP.

Aggregation and redundancy

Link aggregation (IEEE 802.3ad) enables you to bind two or more physical interfaces together to form an aggregated (combined) link. This new link has the bandwidth of all the links combined. If a link in the group fails, traffic is transferred automatically to the remaining interfaces. The only noticeable effect is reduced bandwidth.

This feature is similar to redundant interfaces. The major difference is a redundant interface group only uses one link at a time, where an aggregate link group uses the total bandwidth of the functioning links in the group, up to eight (or more).

An interface is available to be an aggregate interface if:

- It is a physical interface and not a VLAN interface or subinterface.
- It is not already part of an aggregate or redundant interface.
- It is in the same VDOM as the aggregated interface. Aggregate ports cannot span multiple VDOMs.
- It does not have an IP address and is not configured for DHCP or PPPoE.
- It is not referenced in any security policy, VIP, IP Pool, or multicast policy.
- It is not an HA heartbeat interface.
- It is not one of the FortiGate-5000 series backplane interfaces.

When an interface is included in an aggregate interface, it is not listed on the *Network > Interfaces* page. Interfaces still appear in the CLI although configuration for those interfaces do not take effect. You cannot configure the interface individually and it is not available for inclusion in security policies, VIPs, IP pools, or routing.

Sample configuration

This example creates an aggregate interface on a FortiGate-140D POE using ports 3-5 with an internal IP address of 10.1.1.123, as well as the administrative access to HTTPS and SSH.

To create an aggregate interface using the GUI:

1. Go to *Network > Interfaces* and select *Create New > Interface*.
2. For *Interface Name*, enter *Aggregate*.
3. For the *Type*, select *802.3ad Aggregate*.
4. In the physical *Interface Members*, click to add interfaces and select ports 4, 5, and 6.
5. For *Addressing mode*, select *Manual*.
6. For the IP address for the port, enter *10.1.1.123/24*.
7. For *Administrative Access*, select *HTTPS* and *SSH*.
8. Select *OK*.

To create an aggregate interface using the CLI:

```
FG140P3G15800330 (aggregate) # show
config system interface
    edit "aggregate"
        set vdom "root"
        set ip 10.1.1.123 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm radius-acct capwap ftm
        set type aggregate
        set member "port3" "port4" "port5"
        set device-identification enable
        set lldp-transmission enable
        set fortiheartbeat enable
        set role lan
        set snmp-index 45
    next
end
```

Redundancy

In a redundant interface, traffic only goes over one interface at any time. This differs from an aggregated interface where traffic goes over all interfaces for increased bandwidth. This difference means redundant interfaces can have more robust configurations with fewer possible points of failure. This is important in a fully-meshed HA configuration.

An interface is available to be in a redundant interface if:

- It is a physical interface and not a VLAN interface.
- It is not already part of an aggregated or redundant interface.
- It is in the same VDOM as the redundant interface.
- It does not have an IP address and is not configured for DHCP or PPPoE.
- It has no DHCP server or relay configured on it.
- It does not have any VLAN subinterfaces.
- It is not referenced in any security policy, VIP, or multicast policy.
- It is not monitored by HA.
- It is not one of the FortiGate-5000 series backplane interfaces.

When an interface is included in a redundant interface, it is not listed on the *Network > Interfaces* page. You cannot configure the interface individually and it is not available for inclusion in security policies, VIPs, or routing.

Sample configuration

To create a redundant interface using the GUI:

1. Go to *Network > Interfaces* and select *Create New > Interface*.
2. For *Interface Name*, enter *Redundant*.
3. For the *Type*, select *Redundant Interface*.
4. In the physical *Interface Members*, click to add interfaces and select ports 4, 5, and 6.
5. For *Addressing mode*, select *Manual*.
6. For the IP address for the port, enter *10.13.101.100/24*.
7. For *Administrative Access*, select *HTTPS* and *SSH*.
8. Select *OK*.

To create a redundant interface using the CLI:

```
config system interface
    edit "red"
        set vdom "root"
        set ip 10.13.101.100 255.255.255.0
        set allowaccess https http
        set type redundant
        set member "port4" "port5" "port6"
        set device-identification enable
        set role lan
        set snmp-index 9
    next
end
```

VLANs

Virtual Local Area Networks (VLANs) multiply the capabilities of your FortiGate unit and can also provide added network security. VLANs use ID tags to logically separate devices on a network into smaller broadcast domains. These smaller domains forward packets only to devices that are part of that VLAN domain. This reduces traffic and increases network security.

VLANs in NAT mode

In NAT mode, the FortiGate unit functions as a layer-3 device. In this mode, the FortiGate unit controls the flow of packets between VLANs and can also remove VLAN tags from incoming VLAN packets. The FortiGate unit can also forward untagged packets to other networks such as the Internet.

In NAT mode, the FortiGate unit supports VLAN trunk links with IEEE 802.1Q-compliant switches or routers. The trunk link transports VLAN-tagged packets between physical subnets or networks. When you add VLAN subinterfaces to the FortiGate's physical interfaces, the VLANs have IDs that match the VLAN IDs of packets on the trunk link. The FortiGate unit directs packets with VLAN IDs to subinterfaces with matching IDs.

You can define VLAN subinterfaces on all FortiGate physical interfaces. However, if multiple virtual domains are configured on the FortiGate unit, you only have access to the physical interfaces on your virtual domain. The FortiGate unit can tag packets leaving on a VLAN subinterface. It can also remove VLAN tags from incoming packets and add a different VLAN tag to outgoing packets.

Normally in VLAN configurations, the FortiGate unit's internal interface is connected to a VLAN trunk, and the external interface connects to an Internet router that is not configured for VLANs. In this configuration, the FortiGate unit can apply different policies for traffic on each VLAN interface connected to the internal interface, which results in less network traffic and better security.

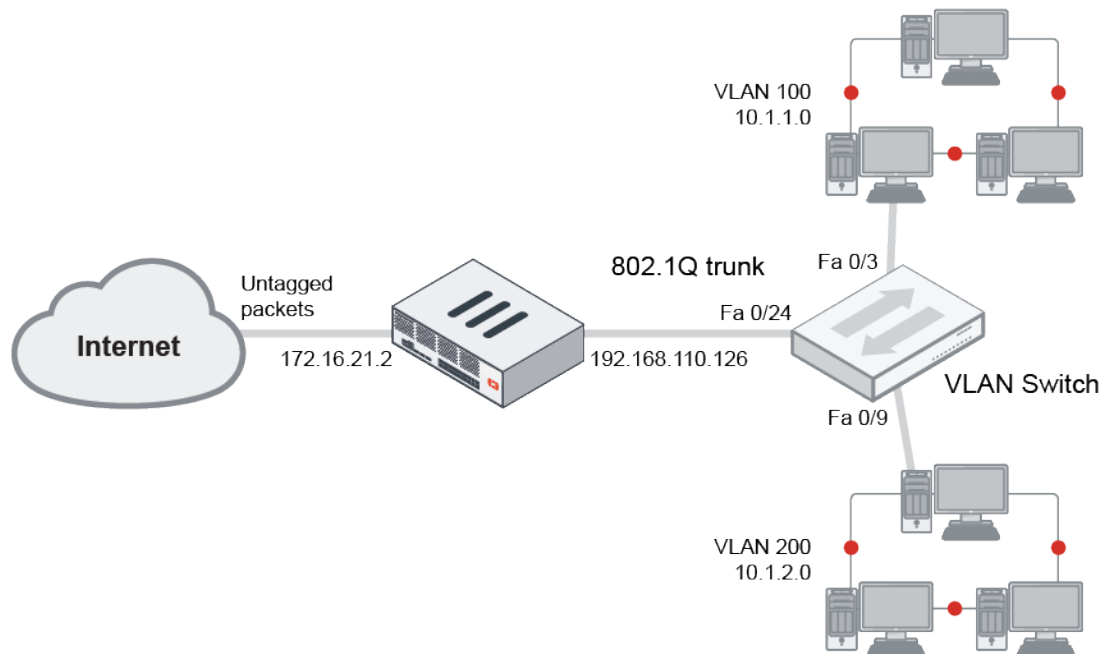
Sample topology

In this example, two different internal VLAN networks share one interface on the FortiGate unit and share the connection to the Internet. This example shows that two networks can have separate traffic streams while sharing a single interface. This configuration can apply to two departments in a single company or to different companies.

There are two different internal network VLANs in this example. VLAN_100 is on the 10.1.1.0/255.255.255.0 subnet, and VLAN_200 is on the 10.1.2.0/255.255.255.0 subnet. These VLANs are connected to the VLAN switch.

The FortiGate internal interface connects to the VLAN switch through an 802.1Q trunk. The internal interface has an IP address of 192.168.110.126 and is configured with two VLAN subinterfaces (VLAN_100 and VLAN_200). The external interface has an IP address of 172.16.21.2 and connects to the Internet. The external interface has no VLAN subinterfaces.

When the VLAN switch receives packets from VLAN_100 and VLAN_200, it applies VLAN ID tags and forwards the packets of each VLAN both to local ports and to the FortiGate unit across the trunk link. The FortiGate unit has policies that allow traffic to flow between the VLANs, and from the VLANs to the external network.



Sample configuration

In this example, both the FortiGate unit and the Cisco 2950 switch are installed and connected and basic configuration has been completed. On the switch, you need access to the CLI to enter commands. No VDOMs are enabled in this example.

General configuration steps include:

1. [Configure the external interface.](#)
2. [Add two VLAN subinterfaces to the internal network interface.](#)
3. [Add firewall addresses and address ranges for the internal and external networks.](#)
4. [Add security policies to allow:](#)
 - the VLAN networks to access each other.
 - the VLAN networks to access the external network.

To configure the external interface:

```
config system interface
    edit external
        set mode static
        set ip 172.16.21.2 255.255.255.0
    end
```


To add VLAN subinterfaces:

```
config system interface
  edit VLAN_100
    set vdom root
    set interface internal
    set type vlan
    set vlanid 100
    set mode static
    set ip 10.1.1.1 255.255.255.0
    set allowaccess https ping
  next
  edit VLAN_200
    set vdom root
    set interface internal
    set type vlan
    set vlanid 200
    set mode static
    set ip 10.1.2.1 255.255.255.0
    set allowaccess https ping
end
```

To add the firewall addresses:

```
config firewall address
  edit VLAN_100_Net
    set type ipmask
    set subnet 10.1.1.0 255.255.255.0
  next
  edit VLAN_200_Net
    set type ipmask
    set subnet 10.1.2.0 255.255.255.0
end
```

To add security policies:

Policies 1 and 2 do not need NAT enabled, but policies 3 and 4 do need NAT enabled.

```
config firewall policy
  edit 1
    set srcintf VLAN_100
    set srcaddr VLAN_100_Net
    set dstintf VLAN_200
    set dstaddr VLAN_200_Net
    set schedule always
    set service ALL
    set action accept
    set nat disable
    set status enable
  next
  edit 2
    set srcintf VLAN_200
    set srcaddr VLAN_200_Net
    set dstintf VLAN_100
    set dstaddr VLAN_100_Net
    set schedule always
```

```
        set service ALL
        set action accept
        set nat disable
        set status enable
    next
    edit 3
        set srcintf VLAN_100
        set srcaddr VLAN_100_Net
        set dstintf external
        set dstaddr all
        set schedule always
        set service ALL
        set action accept
        set nat enable
        set status enable
    next
    edit 4
        set srcintf VLAN_200
        set srcaddr VLAN_200_Net
        set dstintf external
        set dstaddr all
        set schedule always
        set service ALL
        set action accept
        set nat enable
        set status enable
    end
```

VLANs in transparent mode

In transparent mode, the FortiGate unit behaves like a layer-2 bridge but can still provide services such as antivirus scanning, web filtering, spam filtering, and intrusion protection to traffic. Some limitations of transparent mode is that you cannot use SSL VPN, PPTP/L2TP VPN, DHCP server, or easily perform NAT on traffic. The limits in transparent mode apply to IEEE 802.1Q VLAN trunks passing through the unit.

You can insert the FortiGate unit operating in transparent mode into the VLAN trunk without making changes to your network. In a typical configuration, the FortiGate unit internal interface accepts VLAN packets on a VLAN trunk from a VLAN switch or router connected to internal network VLANs. The FortiGate external interface forwards VLAN-tagged packets through another VLAN trunk to an external VLAN switch or router and on to external networks such as the Internet. You can configure the unit to apply different policies for traffic on each VLAN in the trunk.

To pass VLAN traffic through the FortiGate unit, you add two VLAN subinterfaces with the same VLAN ID, one to the internal interface and the other to the external interface. You then create a security policy to permit packets to flow from the internal VLAN interface to the external VLAN interface. If required, create another security policy to permit packets to flow from the external VLAN interface to the internal VLAN interface. Typically in transparent mode, you do not permit packets to move between different VLANs. Network protection features such as spam filtering, web filtering, and anti-virus scanning, are applied through the UTM profiles specified in each security policy, enabling very detailed control over traffic.

When the FortiGate unit receives a VLAN-tagged packet on a physical interface, it directs the packet to the VLAN subinterface with the matching VLAN ID. The VLAN tag is removed from the packet and the FortiGate unit then applies security policies using the same method it uses for non-VLAN packets. If the packet exits the FortiGate unit through a VLAN subinterface, the VLAN ID for that subinterface is added to the packet and the packet is sent to the corresponding physical interface.

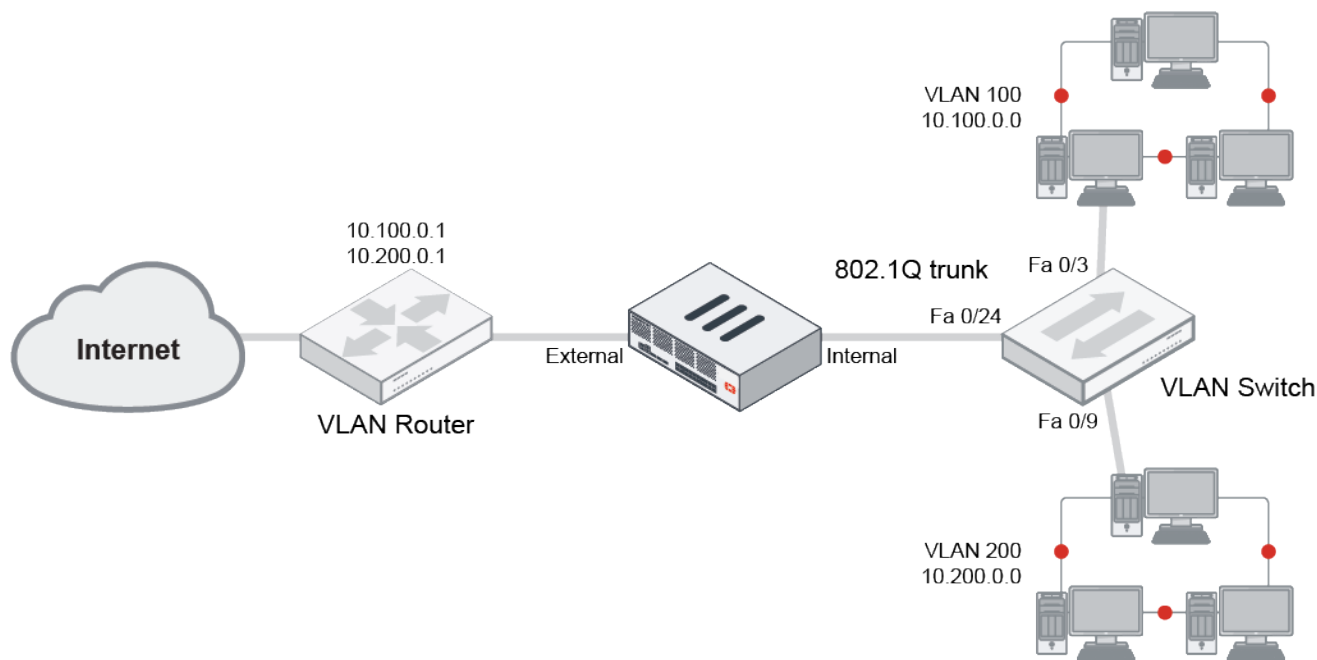
Sample topology

In this example, the FortiGate unit is operating in transparent mode and is configured with two VLANs: one with an ID of 100 and the other with ID 200. The internal and external physical interfaces each have two VLAN subinterfaces, one for VLAN_100 and one for VLAN_200.

The IP range for the internal VLAN_100 network is 10.100.0.0/255.255.0.0, and for the internal VLAN_200 network is 10.200.0.0/255.255.0.0.

The internal networks are connected to a Cisco 2950 VLAN switch which combines traffic from the two VLANs onto one in the FortiGate unit's internal interface. The VLAN traffic leaves the FortiGate unit on the external network interface, goes on to the VLAN switch, and on to the Internet. When the FortiGate unit receives a tagged packet, it directs it from the incoming VLAN subinterface to the outgoing VLAN subinterface for that VLAN.

In this example, we create a VLAN subinterface on the internal interface and another one on the external interface, both with the same VLAN ID. Then we create security policies that allow packets to travel between the VLAN_100_int interface and the VLAN_100_ext interface. Two policies are required: one for each direction of traffic. The same is required between the VLAN_200_int interface and the VLAN_200_ext interface, for a total of four security policies.



Sample configuration

There are two main steps to configure your FortiGate unit to work with VLANs in transparent mode:

1. [Add VLAN subinterfaces.](#)
2. [Add security policies.](#)

You can also configure the protection profiles that manage antivirus scanning, web filtering, and spam filtering.

To add VLAN subinterfaces:

```
config system interface
    edit VLAN_100_int
        set type vlan
```

```
        set interface internal
        set vlanid 100
    next
    edit VLAN_100_ext
        set type vlan
        set interface external
        set vlanid 100
    next
    edit VLAN_200_int
        set type vlan
        set interface internal
        set vlanid 200
    next
    edit VLAN_200_ext
        set type vlan
        set interface external
        set vlanid 200
end
```

To add security policies:

```
config firewall policy
    edit 1
        set srcintf VLAN_100_int
        set srcaddr all
        set dstintf VLAN_100_ext
        set dstaddr all
        set action accept
        set schedule always
        set service ALL
    next
    edit 2
        set srcintf VLAN_100_ext
        set srcaddr all
        set dstintf VLAN_100_int
        set dstaddr all
        set action accept
        set schedule always
        set service ALL
    next
    edit 3
        set srcintf VLAN_200_int
        set srcaddr all
        set dstintf VLAN_200_ext
        set dstaddr all
        set action accept
        set schedule always
        set service ALL
    next
    edit 4
        set srcintf VLAN_200_ext
        set srcaddr all
        set dstintf VLAN_200_int
        set dstaddr all
        set action accept
        set schedule always
```

```
set service ALL  
end
```

Enhanced MAC VLANs

The Media Access Control (MAC) Virtual Local Area Network (VLAN) feature in Linux allows you to configure multiple virtual interfaces with different MAC addresses (and therefore different IP addresses) on a physical interface.

FortiGate implements an enhanced MAC VLAN consisting of a MAC VLAN with bridge functionality. Because each MAC VLAN has a unique MAC address, virtual IP addresses (VIPs) and IP pools are supported, and you can disable Source Network Address Translation (SNAT) in policies.

MAC VLAN cannot be used in a transparent mode virtual domain (VDM). In a transparent mode VDM, a packet leaves an interface with the MAC address of the original source instead of the interface's MAC address. FortiGate implements an enhanced version of MAC VLAN where it adds a MAC table in the MAC VLAN which learns the MAC addresses when traffic passes through.

If you configure a VLAN ID for an enhanced MAC VLAN, it won't join the switch of the underlying interface. When a packet is sent to this interface, a VLAN tag is inserted in the packet and the packet is sent to the driver of the underlying interface. When the underlying interface receives a packet, if the VLAN ID doesn't match, it won't deliver the packet to this enhanced MAC VLAN interface.



When using a VLAN ID, the ID and the underlying interface must be a unique pair, even if they belong to different VDMs. This is because the underlying, physical interface uses the VLAN ID as the identifier to dispatch traffic among the VLAN and enhanced MAC VLAN interfaces.

If you use an interface in an enhanced MAC VLAN, do not use it for other purposes such as a management interface, HA heartbeat interface, or in Transparent VDMs.

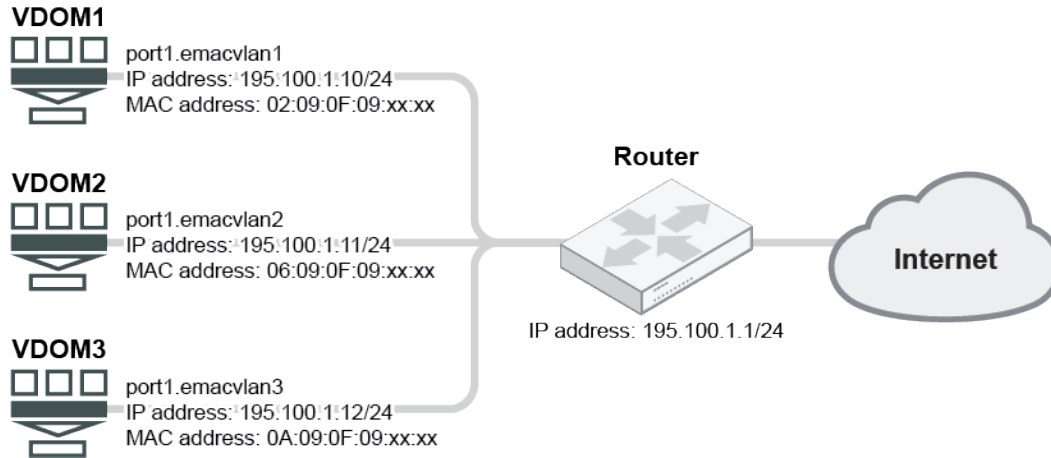
If a physical interface is used by an EMAC VLAN interface, you cannot use it in a Virtual Wire Pair.

In high availability (HA) configurations, enhanced MAC VLAN is treated as a physical interface. It's assigned a unique physical interface ID and the MAC table is synchronized with the secondary devices in the same HA cluster.

Example 1: Enhanced MAC VLAN configuration for multiple VDMs that use the same interface or VLAN

In this example, a FortiGate is connected, through port 1 to a router that's connected to the Internet. Three VDMs share the same interface (port 1) which connects to the same router that's connected to the Internet. Three enhanced MAC VLAN interfaces are configured on port 1 for the three VDMs. The enhanced MAC VLAN interfaces are in the same IP subnet segment and each have unique MAC addresses.

The underlying interface (port 1) can be a physical interface, an aggregate interface, or a VLAN interface on a physical or aggregate interface.



To configure enhanced MAC VLAN for this example in the CLI:

```

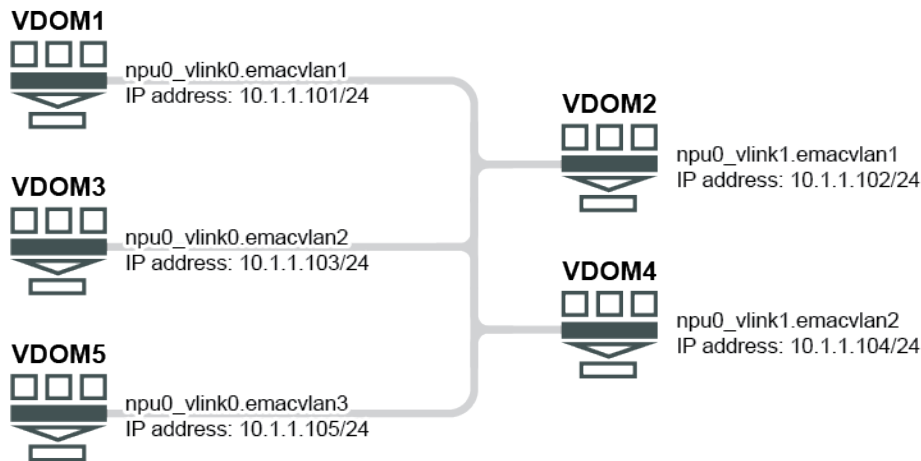
config system interface
  edit port1.emacvlan1
    set vdom VDOM1
    set type emac-vlan
    set interface port1
  next
  edit port 1.emacvlan2
    set vdom VDOM2
    set type emac-vlan
    set interface port1
  next
  edit port1.emacvlan3
    set vdom VDOM3
    set type emac-vlan
    set interface port1
  next
end

```

Example 2: Enhanced MAC VLAN configuration for shared VDOM links among multiple VDOMs

In this example, multiple VDOMs can connect to each other using enhanced MAC VLAN on network processing unit (NPU) virtual link (Vlink) interfaces.

FortiGate VDOM links (NPU-Vlink) are designed to be peer-to-peer connections and VLAN interfaces on NPU Vlink ports use the same MAC address. Connecting more than two VDOMs using NPU Vlinks and VLAN interfaces is not recommended.



To configure enhanced MAC VLAN for this example in the CLI:

```
config system interface
  edit npu0_vlink0.emacvlan1
    set vdom VDOM1
    set type emac-vlan
    set interface npu0_vlink0
  next
  edit npu0_vlink0.emacvlan2
    set vdom VDOM3
    set type emac-vlan
    set interface npu0_vlink0
  next
  edit npu0_vlink1.emacvlan1
    set vdom VDOM2
    set type emac-vlan
    set interface npu0_vlink1
  next
end
```

Example 3: Enhanced MAC VLAN configuration for unique MAC addresses for each VLAN interface on the same physical port

Some networks require a unique MAC address for each VLAN interface when the VLAN interfaces share the same physical port. In this case, the enhanced MAC VLAN interface is used the same way as normal VLAN interfaces.

To configure this, use the `set vlandid` command for the VLAN tag. The VLAN ID and interface must be a unique pair, even if they belong to different VDOMs.

To configure enhanced MAC VLAN:

```
config system interface
  edit <interface-name>
    set type emac-vlan
    set vlandid <VLAN-ID>
    set interface <physical-interface>
  next
end
```

Inter-VDOM routing

VDOM links allow VDOMs to communicate internally without using additional physical interfaces.

Inter-VDOM routing is the communication between VDOMs. VDOM links are virtual interfaces that connect VDOMs. A VDOM link contains a pair of interfaces, each one connected to a VDOM and forming either end of the inter-VDOM connection.

When VDOMs are configured on your FortiGate unit, configuring inter-VDOM routing and VDOM links is like creating a VLAN interface. VDOM links can be managed in either the CLI or in the network interface list in the GUI.



VDOM link does not support traffic offload. If you want to use traffic offload, use NPU-VDOM-LINK.

To configure a VDOM link in the GUI:

1. In the Global VDOM, go to *Network > Interfaces*.
2. Click *Create New > VDOM Link*.
3. Configure the fields, including the *Name*, *Virtual Domain*, IP information, *Administrative Access*, and others, then click *OK*.



By default, VDOM links are created as point-to-point (ppp) links. If required, the link type can be changed in the CLI.

For example, when running OSPF in IPv6, a link-local address is required in order to communicate with OSPF neighbors. For a VDOM link to obtain a link-local address its type must be set to `ethernet`.

To configure a VDOM link in the CLI:

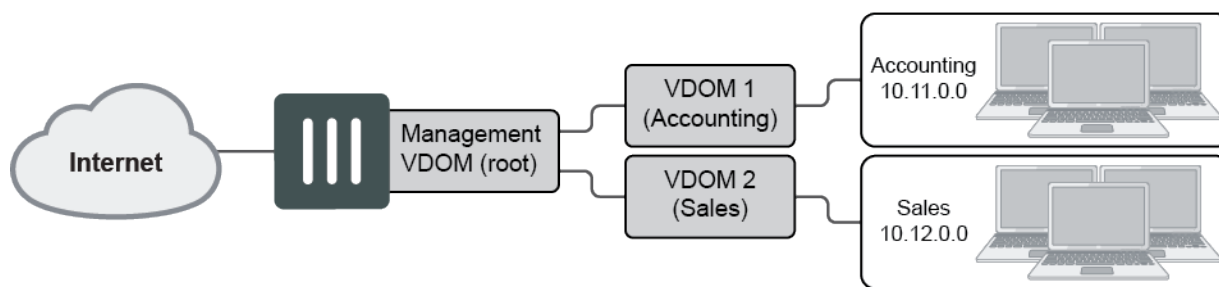
```
config global
  config system vdom-link
    edit "<vdom-link-name>"
      set type {ppp | ethernet}
    next
  end
  config system interface
    edit "<vdom-link-name0>"
      set vdom "<VDOM Name>"
      set type vdom-link
    next
    edit "<vdom-link-name1>"
      set vdom "<VDOM Name>"
      set type vdom-link
    next
  end
end
```


To delete a VDOM link in the GUI:

1. In the Global VDOM, go to *Network > Interfaces*.
2. Select a *VDOM Link* and click *Delete*.

To delete a VDOM link in the CLI:

```
config global
    config system vdom-link
        delete <VDOM-LINK-Name>
    end
end
```

Example

This example shows how to configure a FortiGate unit to use inter-VDOM routing.

Two departments of a company, Accounting and Sales, are connected to one FortiGate. The company uses a single ISP to connect to the Internet.

This example includes the following general steps. We recommend following the steps in the order below.

Create the VDOMs**To enable VDOMs:**

```
config system global
    set vdom-mode multi-vdom
end
```

You will be logged out of the device when VDOM mode is enabled.

To create the Sales and Accounting VDOMs:

```
config global
    config vdom
        edit Accounting
        next
        edit Sales
        next
    end
end
```

Configure the physical interfaces

Next, configure the physical interfaces. This example uses three interfaces on the FortiGate unit: port2 (internal), port3 (DMZ), and port1 (external). Port2 and port3 interfaces each have a department's network connected. Port1 is for all traffic to and from the Internet and uses DHCP to configure its IP address, which is common with many ISPs.

To configure the interfaces:

```
config global
  config system interface
    edit port2
      set alias AccountingLocal
      set vdom Accounting
      set mode static
      set ip 172.100.1.1 255.255.0.0
      set allowaccess https ping ssh
      set description "The accounting dept internal interface"
    next
    edit port3
      set alias SalesLocal
      set vdom Sales
      set mode static
      set ip 192.168.1.1 255.255.0.0
      set allowaccess https ping ssh
      set description "The sales dept. internal interface"
    next
    edit port1
      set alias ManagementExternal
      set vdom root
      set mode dhcp
      set allowaccess https ssh snmp
      set description "The system wide management interface."
    next
  end
end
```

Configure the VDOM links

To complete the connection between each VDOM and the management VDOM, add the two VDOM links. One pair is the Accounting – management link and the other is the Sales – management link.

When configuring inter-VDOM links, you do not have to assign IP addresses to the links unless you are using advanced features such as dynamic routing that require them. Not assigning IP addresses results in faster configuration and more available IP addresses on your networks.

To configure the Accounting and management VDOM link:

```
config global
  config system vdom-link
    edit AccountVlnk
  next
end
config system interface
  edit AccountVlnk0
    set vdom Accounting
```

```
        set ip 11.11.11.2 255.255.255.0
        set allowaccess https ping ssh
        set description "Accounting side of the VDOM link"
    next
    edit AccountVlnk1
        set vdom root
        set ip 11.11.11.1 255.255.255.0
        set allowaccess https ping ssh
        set description "Management side of the VDOM link"
    next
end
end
```

To configure the Sales and management VDOM link:

```
config global
    config system vdom-link
        edit SalesVlnk
            next
        end
    config system interface
        edit SalesVlnk0
            set vdom Sales
            set ip 12.12.12.2 255.255.255.0
            set allowaccess https ping ssh
            set description "Sales side of the VDOM link"
        next
        edit SalesVlnk1
            set vdom root
            set ip 12.12.12.1 255.255.255.0
            set allowaccess https ping ssh
            set description "Management side of the VDOM link"
        next
    end
end
```

Configure the firewall and security profile

With the VDOMs, physical interfaces, and VDOM links configured, the firewall must now be configured to allow the proper traffic. Firewalls are configured per-VDOM, and firewall objects and routes must be created for each VDOM separately.

To configure the firewall policies from AccountingLocal to Internet:

```
config vdom
    edit Accounting
        config firewall policy
            edit 1
                set name "Accounting-Local-to-Management"
                set srcintf port2
                set dstintf AccountVlnk0
                set srcaddr all
                set dstaddr all
                set action accept
                set schedule always
            
```

```
        set service ALL
        set nat enable
    next
end
next
edit root
    config firewall policy
        edit 2
            set name "Accounting-VDOM-to-Internet"
            set srcintf AccountVlnk1
            set dstintf port1
            set srcaddr all
            set dstaddr all
            set action accept
            set schedule always
            set service ALL
            set nat enable
        next
    end
next
end
```

To configure the firewall policies from SalesLocal to the Internet:

```
config vdom
    edit Sales
        config firewall policy
            edit 3
                set name "Sales-local-to-Management"
                set srcintf port3
                set dstintf SalesVlnk0
                set srcaddr all
                set dstaddr all
                set action accept
                set schedule always
                set service ALL
                set nat enable
            next
        end
    next
edit root
    config firewall policy
        edit 4
            set name "Sales-VDOM-to-Internet"
            set srcintf SalesVlnk1
            set dstintf port1
            set srcaddr all
            set dstaddr all
            set action accept
            set schedule always
            set service ALL
            set nat enable
        next
    end
next
end
```

Test the configuration

When the inter-VDOM routing has been configured, test the configuration to confirm proper operation. Testing connectivity ensures that physical networking connections, FortiGate unit interface configurations, and firewall policies are properly configured.

The easiest way to test connectivity is to use the `ping` and `traceroute` commands to confirm the connectivity of different routes on the network.

Test both from AccountingLocal to the internet and from SalesLocal to the internet.

Software switch

A software switch, or soft switch, is a virtual switch that is implemented at the software or firmware level and not at the hardware level. A software switch can be used to simplify communication between devices connected to different FortiGate interfaces. For example, using a software switch, you can place the FortiGate interface connected to an internal network on the same subnet as your wireless interfaces. Then devices on the internal network can communicate with devices on the wireless network without any additional configuration on the FortiGate unit, such as additional security policies.

A software switch can also be useful if you require more hardware ports for the switch on a FortiGate unit. For example, if your FortiGate unit has a 4-port switch, WAN1, WAN2, and DMZ interfaces, and you need one more port, you can create a soft switch that can include the four-port switch and the DMZ interface, all on the same subnet. These types of applications also apply to wireless interfaces, virtual wireless interfaces, and physical interfaces such as those in FortiWiFi and FortiAP units.

Similar to a hardware switch, a software switch functions like a single interface. A soft switch has one IP address and all the interfaces in the software switch are on the same subnet. Traffic between devices connected to each interface are not regulated by security policies, and traffic passing in and out of the switch are controlled by the same policy.

When setting up a software switch, consider the following:

- Ensure you have a back up of the configuration.
- Ensure you have at least one port or connection such as the console port to connect to the FortiGate unit. If you accidentally combine too many ports, you need a way to undo errors.
- The ports that you include must not have any link or relation to any other aspect of the FortiGate unit, such as DHCP servers, security policies, and so on.
- For increased security, you can create a captive portal for the switch to allow only specific user groups access to the resources connected to the switch.

Some of the difference between software and hardware switches are:

Feature	Software switch	Hardware switch
Processing	Packets are processed in software by the CPU.	Packets are processed in hardware by the hardware switch controller, or SPU where applicable.
STP	Not Supported	Supported
Wireless SSIDs	Supported	Not Supported
Intra-switch traffic	Allowed by default. Can be explicitly set to require a policy.	Allowed by default.

To create a software switch in the GUI:

1. Go to *Network > Interfaces*.
2. Click *Create New > Interface*.
3. Set *Type* to *Software Switch*.
4. Configure the *Interface Name*, *Virtual Domain*, *Interface Members*, and other fields.
To add an interface to a software switch, it cannot be referenced by an existing configuration and its IP address must be set to 0.0.0.0/0.0.0.0.
5. Click *OK*.

To create a software switch in the CLI:

```
config system switch-interface
    edit <switch-name>
        set type switch
        set member <interface_list>
    next
end
config system interface
    edit <switch_name>
        set ip <ip_address>
        set allowaccess https ssh ping
    next
end
```

To add an interface to a software switch, it cannot be referenced by an existing configuration and its IP address must be set to 0.0.0.0/0.0.0.0.

Example

For this example, the wireless interface (WiFi) needs to be on the same subnet as the DMZ1 interface to facilitate wireless syncing from an iPhone and a local computer. Because syncing between two subnets is problematic, putting both interfaces on the same subnet the syncing will work. The software switch will accomplish this.

1. Clear the interfaces and back up the configuration.
 - a. Ensure the interfaces are not used for other security policy or for other use on the FortiGate unit.
 - b. Check the WiFi and DMZ1 ports to ensure DHCP is not enabled on the interface and that there are no other dependencies on these interfaces.
 - c. Save the current configuration so that if something doesn't work, recovery can be quick.
2. Merge the interfaces.
Merge the WiFi port and DMZ1 port to create a software switch named `synchro` with an IP address of 10.10.21.12. Use the following CLI commands to create the switch, add the IP, and then set the administrative access for HTTPS, SSH and Ping.

```
config system switch-interface
    edit synchro
        set type switch
        set member dmz1 wifi
    next
end
config system interface
    edit synchro
```

```

set ip 10.10.21.12
set allowaccess https ssh ping
next
end

```

When the soft switch is set up, you now add security policies, DHCP servers, and any other configuration you normally do to configure interfaces on the FortiGate unit.

Hardware switch

A hardware switch is a virtual switch interface that groups different ports together so that the FortiGate can use the group as a single interface. Supported FortiGate models have a default hardware switch called either *internal* or *lan*. The hardware switch is supported by the chipset at the hardware level.

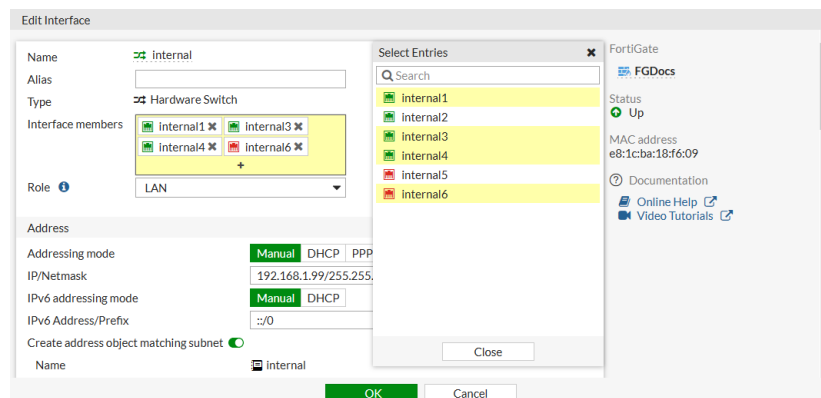
Ports that are connected to the same hardware switch behave like they are on the same physical switch in the same broadcast domain. Ports can be removed from a hardware switch and assigned to another switch or used as standalone interfaces.

Some of the difference between hardware and software switches are:

Feature	Hardware switch	Software switch
Processing	Packets are processed in hardware by the hardware switch controller, or SPU where applicable.	Packets are processed in software by the CPU.
STP	Supported	Not Supported
Wireless SSIDs	Not Supported	Supported
Intra-switch traffic	Allowed by default.	Allowed by default. Can be explicitly set to require a policy.

To change the ports in a hardware switch in the GUI:

1. Go to *Network > Interface* and edit the hardware switch.
2. Click inside the *Interface members* field.



3. Select interfaces to add or remove them from the hardware switch, then click *Close*.

To add an interface to a hardware switch, it cannot be referenced by an existing configuration and its IP address must be set to 0.0.0.0/0.0.0.0.

4. Click OK.

Removed interfaces will now be listed as standalone interfaces in the *Physical Interface* section.

To remove ports from a hardware switch in the CLI:

```
config system virtual-switch
  edit "internal"
    config port
      delete internal2
      delete internal5
    end
  next
end
```

To add ports to a hardware switch in the CLI:

```
config system virtual-switch
  edit "internal"
    set physical-switch "sw0"
    config port
      edit "internal1"
      next
      edit "internal3"
      next
      edit "internal4"
      next
      edit "internal6"
      next
    end
  next
end
```

To add an interface to a hardware switch, it cannot be referenced by an existing configuration and its IP address must be set to 0.0.0.0/0.0.0.0.

Zone

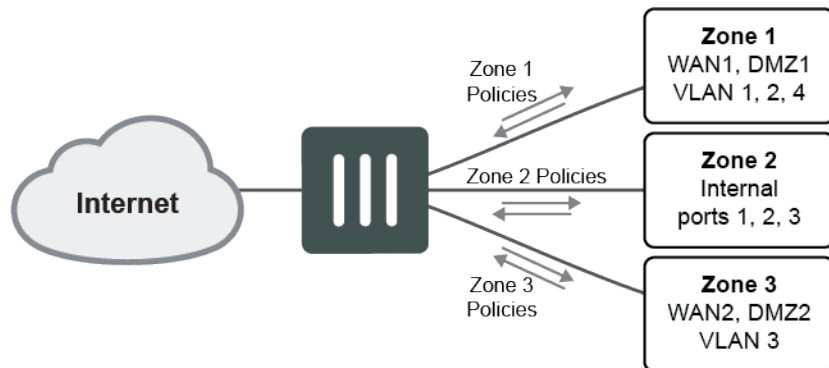
Zones are a group of one or more physical or virtual FortiGate interfaces that you can apply security policies to control inbound and outbound traffic. Grouping interfaces and VLAN subinterfaces into zones simplifies the creation of security policies where a number of network segments can use the same policy settings and protection profiles.

When you add a zone, you select the names of the interfaces and VLAN subinterfaces to add to the zone. Each interface still has its own address. Routing is still done between interfaces, that is, routing is not affected by zones. You can use security policies to control the flow of intra-zone traffic.

For example, in the sample configuration below, the network includes three separate groups of users representing different entities on the company network. While each group has its own set of ports and VLANs in each area, they can all use the same security policy and protection profiles to access the Internet. Rather than the administrator making nine separate security policies, he can make administration simpler by adding the required interfaces to a zone and creating three policies.

Sample configuration

You can configure policies for connections to and from a zone but not between interfaces in a zone. For this example, you can create a security policy to go between zone 1 and zone 3, but not between WAN2 and WAN1, or WAN1 and DMZ1.



To create a zone in the GUI:

1. Go to *Network > Interfaces*.



If VDOMs are enabled, go to the VDOM to create a zone.

2. Click *Create New > Zone*.
3. Configure the *Name* and add the *Interface Members*.

To configure a zone to include the internal interface and a VLAN using the CLI:

```

config system zone
  edit Zone_1
    set interface internal VLAN_1
    set intrazone deny/allow
  next
end

```

Using zone in a firewall policy

To configure a firewall policy to allow any interface to access the Internet using the CLI:

```

config firewall policy
  edit 2
    set name "2"
    set srcintf "Zone_1"
    set dstintf "port15"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
  
```

```
        set nat enable
    next
end
```

Intra-zone traffic

In the zone configuration you can set `intrazone deny` to prohibit the different interfaces in the same zone to talk to each other.

For example, if you have ten interfaces in your zone and the `intrazone` setting is `deny`. You now want to allow traffic between a very small number of networks on different interfaces that are part of the zone but you do not want to disable the intra-zone blocking.

In this example, the zone VLANs are defined as: 192.168.1.0/24, 192.168.2.0/24, ... 192.168.10.0/24.

This policy allows traffic from 192.168.1.x to 192.168.2.x even though they are in the same zone and intra-zone blocking is enabled. The intra-zone blocking acts as a default deny rule and you have to specifically override it by creating a policy within the zone.

To enable intra-zone traffic, create the following policy:

Source Interface	Zone-name, e.g., Vlans
Source Address	192.168.1.0/24
Destination	Zone-name (same as Source Interface, i.e., Vlans)
Destination Address	192.168.2.0/24

Virtual Wire Pair

A virtual wire pair consists of two interfaces that do not have IP addressing and are treated like a transparent mode VDOM. All traffic received by one interface in the virtual wire pair can only be forwarded to the other interface, provided a virtual wire pair firewall policy allows this traffic. Traffic from other interfaces cannot be routed to the interfaces in a virtual wire pair. Redundant and 802.3ad aggregate (LACP) interfaces can be included in a virtual wire pair.

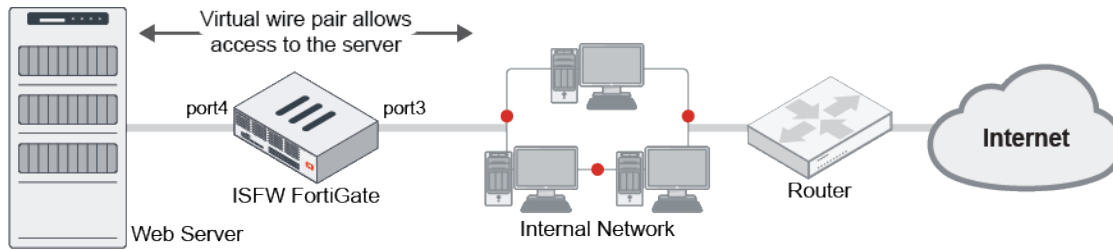
Virtual wire pairs are useful for a typical topology where MAC addresses do not behave normally. For example, port pairing can be used in a Direct Server Return (DSR) topology where the response MAC address pair may not match the request's MAC address pair.

Example

In this example, a virtual wire pair (port3 and port4) makes it easier to protect a web server that is behind a FortiGate operating as an Internal Segmentation Firewall (ISFW). Users on the internal network access the web server through the ISFW over the virtual wire pair.



Interfaces used in a virtual wire pair cannot be used to access the ISFW FortiGate. Before creating a virtual wire pair, make sure you have a different port configured to allow admin access using your preferred protocol.



To add a virtual wire pair using the CLI:

```
config system virtual-wire-pair
  edit "VWP-name"
    set member "port3" "port4"
    set wildcard-vlan disable
  next
end
```

To add a virtual wire pair using the GUI:

1. Go to *Network > Interfaces*.
2. Click *Create New > Virtual Wire Pair*.
3. Select the *Interface Members* to add to the virtual wire pair.
These interfaces cannot be part of a switch, such as the default LAN/internal interface.
4. If required, enable *Wildcard VLAN* and set the *VLAN Filter*.
5. Click *OK*.

To create a virtual wire pair policy using the CLI:

```
config firewall policy
  edit 1
    set name "VWP-Policy"
    set srcintf "port3" "port4"
    set dstintf "port3" "port4"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set fsso disable
  next
end
```

To create a virtual wire pair policy using the GUI:

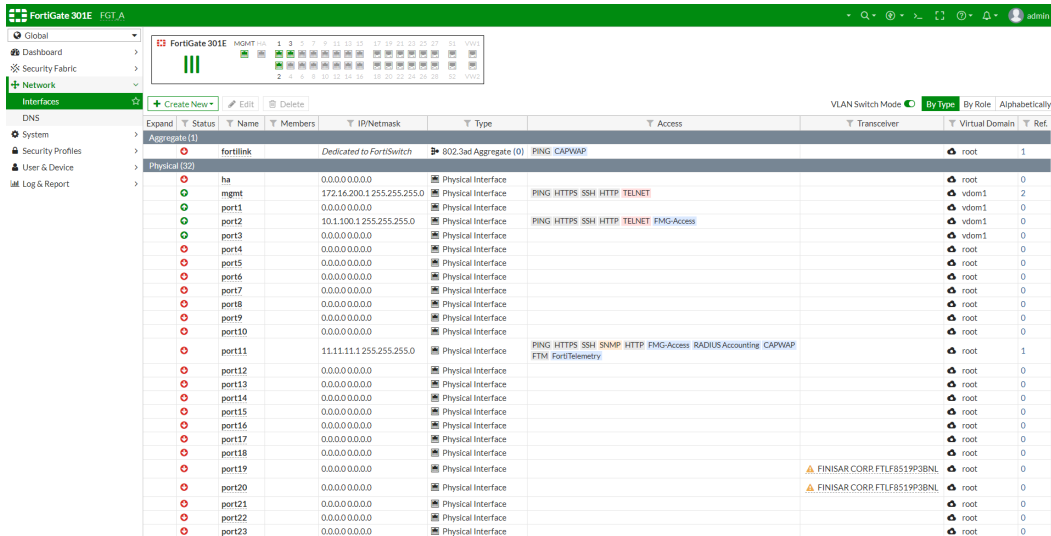
1. Go to *Policy & Objects > IPv4 Virtual Wire Pair Policy*.
2. Click *Create New*.
3. Select the direction that traffic is allowed to flow.
4. Configure the other fields.
5. Click *OK*.

Virtual switch support for FortiGate 300E series

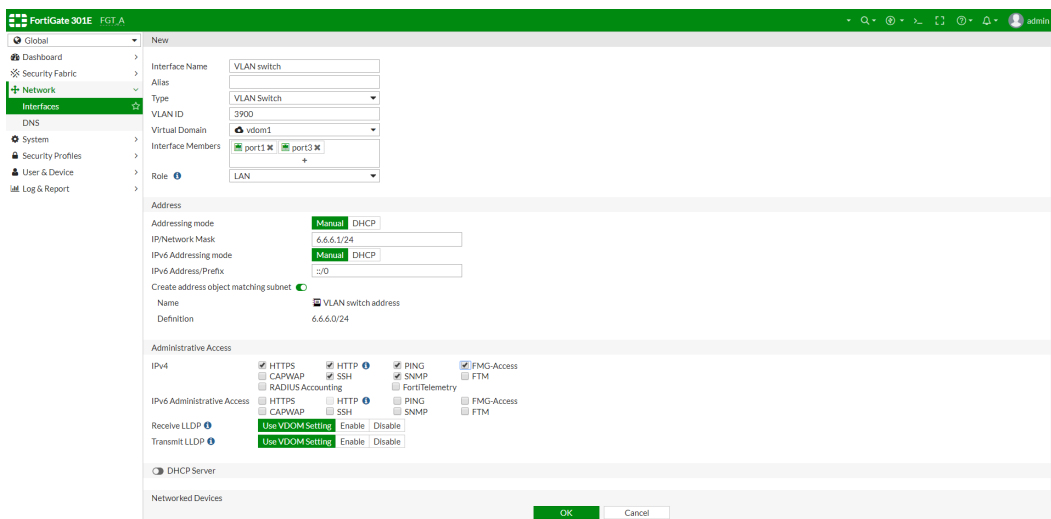
On the FortiGate 300E series, switch ports can be assigned to different VLANs.

To create a VLAN switch in the GUI:

1. Go to **Network > Interfaces** and enable **VLAN Switch Mode**.



2. Click **Create New > Interface**.
3. Enter an interface name and configure the following:
 - a. For **Type**, select **VLAN Switch**.
 - b. (Optional) Enter a **VLAN ID** (range is 3900–3999).
 - c. If applicable, select a **Virtual Domain**.
 - d. Add the **Interface Members**.
 - e. Configure the **Address** and **Administrative Access** settings as needed.
4. Click **OK**.



The new VLAN switch is visible in the interface table:

Expand	Status	Name	Members	IP Netmask	Type	Access	Transceiver	Virtual Domain	Ref.
		port12		0.0.0.0/0.0.0	Physical Interface			root	0
		port13		0.0.0.0/0.0.0	Physical Interface			root	0
		port14		0.0.0.0/0.0.0	Physical Interface			root	0
		port15		0.0.0.0/0.0.0	Physical Interface			root	0
		port16		0.0.0.0/0.0.0	Physical Interface			root	0
		port17		0.0.0.0/0.0.0	Physical Interface			root	0
		port18		0.0.0.0/0.0.0	Physical Interface			root	0
		port19		0.0.0.0/0.0.0	Physical Interface			root	0
		port20		0.0.0.0/0.0.0	Physical Interface			root	0
		port21		0.0.0.0/0.0.0	Physical Interface			root	0
		port22		0.0.0.0/0.0.0	Physical Interface			root	0
		port23		0.0.0.0/0.0.0	Physical Interface			root	0
		port24		0.0.0.0/0.0.0	Physical Interface			root	0
		port25		0.0.0.0/0.0.0	Physical Interface			root	0
		port26		0.0.0.0/0.0.0	Physical Interface			root	0
		port27		0.0.0.0/0.0.0	Physical Interface			root	0
		port28		0.0.0.0/0.0.0	Physical Interface			root	0
		s1		One-Arm Sniffer	Physical Interface			root	1
		s2		One-Arm Sniffer	Physical Interface			root	1
		VDOM Link (0)			NPU VDOM Link			root, root	0
		Virtual Wire Pair (0)			Virtual Wire Pair			root	0
		pair-1			Virtual Wire Pair			root	0
		VLAN Switch (1)							
		VLAN switch (VLAN ID: 3900)		6.6.6.1/255.255.255.0	VLAN Switch (2)	PING HTTPS SSH SNMP HTTP PKG Access		vdom1	1

To create a VLAN switch in the CLI:

1. Enable VLAN switch mode:

```
config system global
    set virtual-switch-vlan enable
end
```

2. Create the VLAN switch. Optionally, you can assign an ID to the VLAN: The default ID is 0. You can use the default ID, or you can assign an ID to the VLAN (3900–3999).

```
config system virtual-switch
    edit "VLAN switch"
        set physical-switch "sw0"
        set vlan 3900
    config port
        edit "port1"
            next
        edit "port3"
            next
        end
    next
end
```

3. Configure the VLAN switch interface:

```
config system interface
    edit "VLAN switch"
        set vdom "vdom1"
        set ip 6.6.6.1 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm
        set type hard-switch
        set snmp-index 15
    next
end
```

4. (Optional) Create a trunk interface:

```
config system interface
    edit port2
```

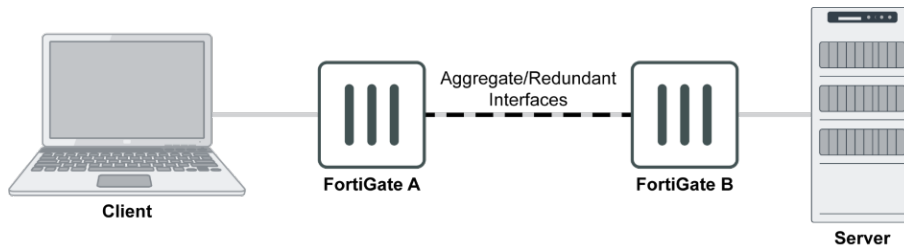
```

        set trunk enable
    next
end

```

Failure detection for aggregate and redundant interfaces

When an aggregate or redundant interface goes down, the corresponding fail-alert interface changes to down. When an aggregate or redundant interface comes up, the corresponding fail-alert interface changes to up.



Fail-detect for aggregate and redundant interfaces can be configured using the CLI.

To configure an aggregate interface so that port3 goes down with it:

```

config system interface
    edit "aggl"
        set vdom "root"
        set fail-detect enable
        set fail-alert-method link-down
        set fail-alert-interfaces "port3"
        set type aggregate
        set member "port1" "port2"
    next
end

```

To configure a redundant interface so that port4 goes down with it:

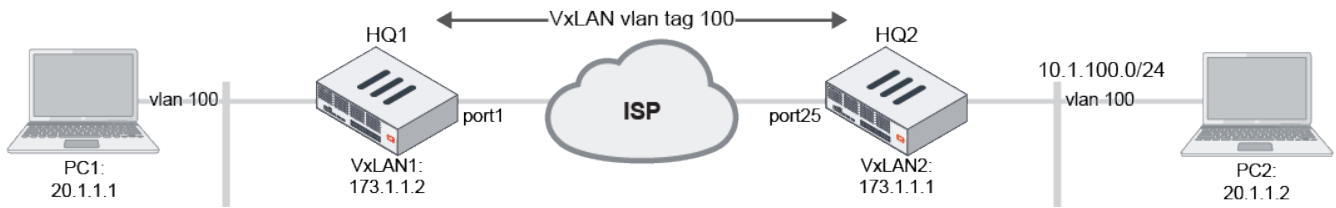
```

config system interface
    edit "red1"
        set vdom "root"
        set fail-detect enable
        set fail-alert-method link-down
        set fail-alert-interfaces "port4"
        set type redundant
        set member "port1" "port2"
    next
end

```

VLAN inside VXLAN

VLANs can be assigned to VXLAN interfaces. In a data center network where VXLAN is used to create an L2 overlay network and for multitenant environments, a customer VLAN tag can be assigned to VXLAN interface. This allows the VLAN tag from VLAN traffic to be encapsulated within the VXLAN packet.



To configure VLAN inside VXLAN on HQ1:

1. Configure VXLAN:

```
config system vxlan
  edit "vxlan1"
    set interface port1
    set vni 1000
    set remote-ip 173.1.1.1
  next
end
```

2. Configure system interface:

```
config system interface
  edit vlan100
    set vdom root
    set vlanid 100
    set interface dmz
  next
  edit vxlan100
    set type vlan
    set vlanid 100
    set vdom root
    set interface vxlan1
  next
end
```

3. Configure software-switch:

```
config system switch-interface
  edit sw1
    set vdom root
    set member vlan100 vxlan100
    set intra-switch-policy implicit
  next
end
```



The default `intra-switch-policy implicit` behavior allows traffic between member interfaces within the switch. Therefore, it is not necessary to create firewall policies to allow this traffic.



Instead of creating a software-switch, it is possible to use a virtual-wire-pair as well. See [Virtual Wire Pair with VXLAN on page 347](#)

To configure VLAN inside VXLAN on HQ2:

1. Configure VXLAN:

```
config system vxlan
edit "vxlan2"
set interface port25
set vni 1000
set remote-ip 173.1.1.2
next
end
```

2. Configure system interface:

```
config system interface
edit vlan100
set vdom root
set vlanid 100
set interface port20
next
edit vxlan100
set type vlan
set vlanid 100
set vdom root
set interface vxlan2
next
end
```

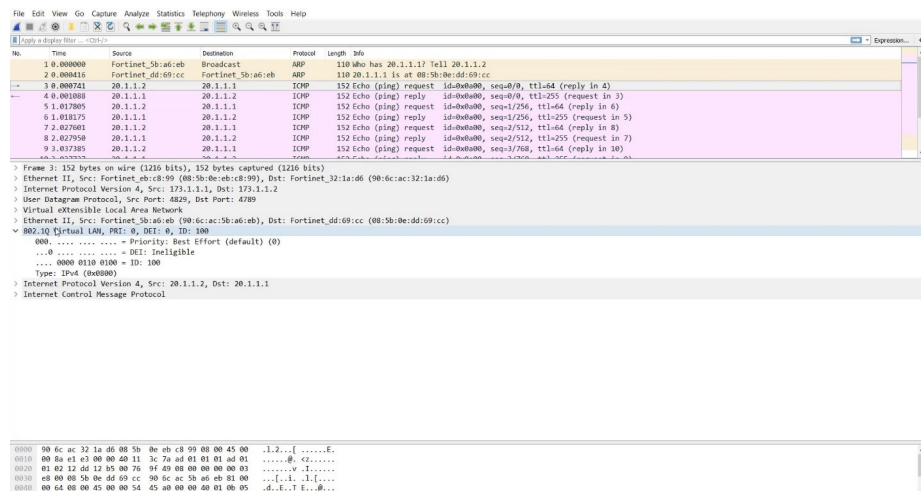
3. Configure software-switch:

```
config system switch-interface
edit sw1
set vdom root
set member vlan100 vxlan100
next
end
```

To verify the configuration:

Ping PC1 from PC2.

The following is captured on HQ2:

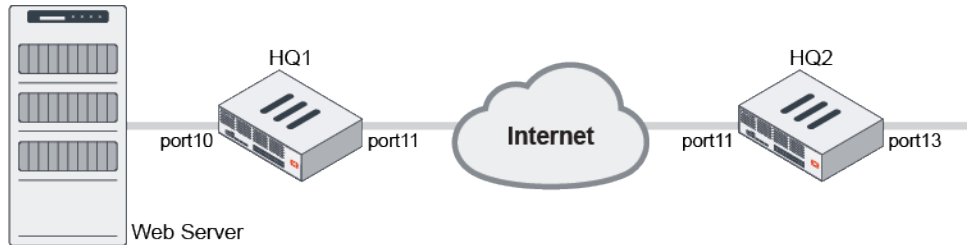


This captures the VXLAN traffic between 172.1.1.1 and 172.1.1.2 with the VLAN 100 tag inside.

Virtual Wire Pair with VXLAN

Virtual wire pairs can be used with VXLAN interfaces.

In this examples, VXLAN interfaces are added between FortiGate HQ1 and FortiGate HQ2, a virtual wire pair is added in HQ1, and firewall policies are created on both HQ1 and HQ2.



To create VXLAN interface on HQ1:

```

config system interface
    edit "port11"
        set vdom "root"
        set ip 10.2.2.1 255.255.255.0
        set allowaccess ping https ssh snmp telnet
    next
end
config system vxlan
    edit "vxlan1"
        set interface "port11"
        set vni 1000
        set remote-ip "10.2.2.2"
    next
end

```

To create VXLAN interface on HQ2:

```

config system interface
    edit "port11"
        set vdom "root"
        set ip 10.2.2.2 255.255.255.0
        set allowaccess ping https ssh snmp http
    next
end
config system vxlan
    edit "vxlan1"
        set interface "port11"
        set vni 1000
        set remote-ip "10.2.2.1"
    next
end
config system interface
    edit "vxlan1"
        set vdom "root"
        set ip 10.1.100.2 255.255.255.0
        set allowaccess ping https ssh snmp
    next
end

```

```
    next
end
```

To create a virtual wire pair on HQ1:

```
config system virtual-wire-pair
    edit "vwp1"
        set member "port10" "vxlan1"
    next
end
```

To create a firewall policy on HQ1:

```
config firewall policy
    edit 5
        set name "vxlan-policy"
        set srcintf "port10" "vxlan1"
        set dstintf "port10" "vxlan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
        set webfilter-profile "default"
        set dnsfilter-profile "default"
        set ips-sensor "default"
        set application-list "default"
        set fsso disable
    next
end
```

To create a firewall policy on HQ2:

```
config firewall policy
    edit 5
        set name "1"
        set srcintf "port13"
        set dstintf "vxlan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set fsso disable
        set nat enable
    next
end
```

Interface MTU packet size

Changing the maximum transmission unit (MTU) on FortiGate interfaces changes the size of transmitted packets. Most FortiGate device's physical interfaces support jumbo frames that are up to 9216 bytes, but some only support 9000 or 9204 bytes.

To avoid fragmentation, the MTU should be the same as the smallest MTU in all of the networks between the FortiGate and the destination. If the packets sent by the FortiGate are larger than the smallest MTU, then they are fragmented, slowing down the transmission. Packets with the DF flag set in the IPv4 header are dropped and not fragmented.

On many network and endpoint devices, the path MTU is used to determine the smallest MTU and to transmit packets within that size.

- ASIC accelerated FortiGate interfaces, such as NP6, NP7, and SOC4 (np6xlite), support MTU sizes up to 9216 bytes.
- Some small desktop FortiGate models, such as the 30E and 50E, and FortiGate Rugged models, such as the 30D and 35D, support MTU sizes up to 1500 bytes.
- FortiGate VMs can have varying maximum MTU sizes, depending on the underlying interface and driver.
- Virtual interfaces, such as VLAN interfaces, inherit their MTU size from their parent interface.

To verify the supported MTU size:

```
config system interface
    edit <interface>
        set mtu-override enable
        set mtu ?
            <integer>      Maximum transmission unit (<min>--<max>)
    next
end
```

To change the MTU size:

```
config system interface
    edit <interface>
        set mtu-override enable
        set mtu <max bytes>
    next
end
```

Maximum MTU size on a path

To manually test the maximum MTU size on a path, you can use the ping command on a Windows computer.

For example, you can send ICMP packets of a specific size with a DF flag, and iterate through increasing sizes until the ping fails.

- The `-f` option specifies the Do not Fragment (DF) flag.
- The `-l` option specifies the length, in bytes, of the Data field in the echo Request messages. This does not include the 8 bytes for the ICMP header and 20 bytes for the IP header. Therefore, if the maximum MTU is 1500 bytes, then the maximum supported data size is: $1500 - 8 - 20 = 1472$ bytes.

To determine the maximum MTU size on a path:

1. In Windows command prompt, try a likely MTU size:

```
>ping 4.2.2.1 -l 1472 -f
```

```
Pinging 4.2.2.1 with 1472 bytes of data:
Reply from 4.2.2.1: bytes=1472 time=41ms TTL=52
Reply from 4.2.2.1: bytes=1472 time=42ms TTL=52
Reply from 4.2.2.1: bytes=1472 time=103ms TTL=52
Reply from 4.2.2.1: bytes=1472 time=38ms TTL=52

Ping statistics for 4.2.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 38ms, Maximum = 103ms, Average = 56ms
```

2. Increase the size and try the ping again:

```
>ping 4.2.2.1 -l 1473 -f
```

```
Pinging 4.2.2.1 with 1473 bytes of data:
Request timed out.
```

```
Ping statistics for 4.2.2.1:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
```

The second test fails, so the maximum MTU size on the path is 1472 bytes + 8-byte ICMP header + 20-byte IP header = 1500 bytes

Maximum segment size

The TCP maximum segment size (MSS) is the maximum amount of data that can be sent in a TCP segment. The MSS is the MTU size of the interface minus the 20 byte IP header and 20 byte TCP header. By reducing the TCP MSS, you can effectively reduce the MTU size of the packet.

The TCP MSS can be configured in a firewall policy, or directly on an interface.

To configure the MSS in a policy:

```
config firewall policy
    edit <policy ID>
        set srcintf "internal"
        set dstintf "wan1"
        set srcaddr "10.10.10.6"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set tcp-mss-sender 1448
        set tcp-mss-receiver 1448
    next
end
```

To configure the MSS on an interface:

```
config system interface
    edit "wan2"
        set vdom "root"
        set mode dhcp
        set allowaccess ping fgfm
        set type physical
    end
```

```

    set tcp-mss 1448
    set role wan
next
end

```

One-arm sniffer

You can use a one-arm sniffer to configure a physical interface as a one-arm intrusion detection system (IDS). Traffic sent to the interface is examined for matches to the configured security profile. The matches are logged, and then all received traffic is dropped. Sniffing only reports on attacks; it does not deny or influence traffic.

You can also use the one-arm sniffer to configure the FortiGate to operate as an IDS appliance to sniff network traffic for attacks without actually processing the packets. To configure a one-arm IDS, enable sniffer mode on a physical interface and connect the interface to the SPAN port of a switch or a dedicated network tap that can replicate the traffic to the FortiGate.

To assign an interface as a sniffer interface in the GUI, go to *Network > Interfaces* and edit the interface. For *Addressing mode*, select *One-Arm Sniffer*.

If the option is not available, the interface is in use. Ensure that the interface is not selected in any firewall policies, routes, virtual IPs, or other features where a physical interface is specified. The option does not appear if the role is set to WAN. Ensure the role is set to LAN, DMZ, or undefined.

The following table lists some of the one-arm sniffer settings you can configure:

Field	Description
Filters	<p>Enable this setting to include filters that define a more granular sniff of network traffic. Select specific hosts, ports, VLANs, and protocols.</p> <p>In all cases, enter a number or range for the filter type. The standard protocols are:</p> <ul style="list-style-type: none"> • UDP: 17 • TCP: 6 • ICMP: 1
Include IPv6 Packets	If the network is running IPv4 and IPv6 addresses, enable this setting to sniff both types; otherwise, the FortiGate will only sniff IPv4 traffic.
Include Non-IPv6 Packets	Enable this setting for a more intense content scan of the traffic.
Security Profiles	<p>The following profiles are configurable in the GUI and CLI:</p> <ul style="list-style-type: none"> • Antivirus • Web filter • Application control • IPS <p>The following profiles are only configurable in the CLI:</p> <ul style="list-style-type: none"> • Email filter • DLP • IPS DoS

CPU usage and packet loss

Traffic scanned on the one-arm sniffer interface is processed by the CPU, even if there is an SPU, such as NPU or CP, present. The one-arm sniffer may cause higher CPU usage and perform at a lower level than traditional inline scanning, which uses NTurbo or CP to accelerate traffic when present.

The absence of high CPU usage does not indicate the absence of packet loss. Packet loss may occur due to the capacity of the TAP devices hitting maximum traffic volume during mirroring, or on the FortiGate when the kernel buffer size is exceeded and it is unable to handle bursts of traffic.

DNS

Domain name system (DNS) is used by devices to locate websites by mapping a domain name to a website's IP address.

A FortiGate can serve different roles based on user requirements:

- A FortiGate can control what DNS server a network uses.
- A FortiGate can function as a DNS server.

FortiGuard Dynamic DNS (DDNS) allows a remote administrator to access a FortiGate's Internet-facing interface using a domain name that remains constant even when its IP address changes.

FortiOS supports DNS configuration for both IPv4 and IPv6 addressing. When a user requests a website, the FortiGate looks to the configured DNS servers to provide the IP address of the website in order to know which server to contact to complete the transaction.

The FortiGate queries the DNS servers whenever it needs to resolve a domain name into an IP address, such as for NTP or web servers defined by their domain names.

The following topics provide information about DNS:

- [Important DNS CLI commands on page 352](#)
- [DNS domain list on page 353](#)
- [FortiGate DNS server on page 355](#)
- [DDNS on page 357](#)
- [DNS latency information on page 360](#)
- [DNS over TLS on page 362](#)
- [DNS troubleshooting on page 362](#)

Important DNS CLI commands

DNS settings can be configured with the following CLI command:

```
config system dns
    set primary <ip_address>
    set secondary <ip_address>
    set dns-over-tls {enable | disable | enforce}
    set ssl-certificate <string>
```

```
set domain <domains>
set ip6-primary <ip6_address>
set ip6-secondary <ip6_address>
set timeout <integer>
set retry <integer>
set dns-cache-limit <integer>
set dns-cache-ttl <integer>
set cache-notfound-responses {enable | disable}
set source-ip <class_ip>
end
```

For a FortiGate with multiple logical CPUs, you can set the DNS process number from 1 to the number of logical CPUs. The default DNS process number is 1.

```
config system global
    set dnsproxy-worker-count <integer>
end
```

dns-over-tls

DNS over TLS (DoT) is a security protocol for encrypting and wrapping DNS queries and answers via the Transport Layer Security (TLS) protocol. It can be enabled, disabled, or enforced:

- **disable:** Disable DNS over TLS (default).
- **enable:** Use TLS for DNS queries if TLS is available.
- **enforce:** Use only TLS for DNS queries. Does not fall back to unencrypted DNS queries if TLS is unavailable.

For more information, see [DNS over TLS on page 362](#).

cache-notfound-responses

When enabled, any DNS requests that are returned with `NOT FOUND` can be stored in the cache. The DNS server is not asked to resolve the host name for `NOT FOUND` entries. By default, this option is disabled.

dns-cache-limit

Set the number of DNS entries that are stored in the cache (0 to 4294967295, default = 5000). Entries that remain in the cache provide a quicker response to requests than going out to the Internet to get the same information.

dns-cache-ttl

The duration that the DNS cache retains information, in seconds (60 to 86400 (1 day), default = 1800).

DNS domain list

You can configure up to eight domains in the DNS settings using the GUI or the CLI.

When a client requests a URL that does not include an FQDN, FortiOS resolves the URL by traversing through the DNS domain list and performing a query for each domain until the first match is found.

By default, FortiGate uses FortiGuard's DNS servers:

- Primary: 208.91.112.53
- Secondary: 208.91.112.52

You can also customize the DNS timeout time and the number of retry attempts.

To configure a DNS domain list in the GUI:

1. Go to *Network > DNS*.
2. Set *DNS Servers* to *Specify*.
3. Configure the primary and secondary DNS servers as needed.
4. In the *Local Domain Name* field, enter the first domain (*sample.com* in this example).
5. Click the + to add more domains (*example.com* and *domainname.com* in this example). You can enter up to eight domains.

DNS Settings

DNS Servers
 Use FortiGuard Servers: **Specify**
 Primary DNS Server: 172.16.200.1
 Secondary DNS Server:
 Local Domain Name: sample.com, example.com, domainname.com

DNS over TLS
 Disable | Enable | Enforce

Dynamically Obtained DNS Servers

Interface	DNS Server
wan1	208.91.112.53
wan2	208.91.112.52

IPv6 DNS Settings
 Primary DNS Server: ::
 Secondary DNS Server: ::

Apply

DNS Servers
 208.91.112.53 4,880 ms
 208.91.112.52 11,190 ms

Acquired DNS Servers
 10 ms

Setup guides
[DNS local domain list](#)
[Using FortiGate as a DNS server](#)
[FortiGuard DDNS](#)

Documentation
[Online Help](#)
[Video Tutorials](#)

6. Configure additional DNS settings as needed.
7. Click *Apply*.

To configure a DNS domain list in the CLI:

```
config system dns
    set primary 172.16.200.1
    set domain "sample.com" "example.com" "domainname.com"
end
```

Verify the DNS configuration

In the following example, the local DNS server has the entry for *host1* mapped to the FQDN of *host1.sample.com*, and the entry for *host2* is mapped to the FQDN of *host2.example.com*.

To verify that the DNS domain list is configured:

1. Open Command Prompt.
2. Enter `ping host1`.

The system returns the following response:

```
PING host1.sample.com (1.1.1.1): 56 data bytes
```


As the request does not include an FQDN, FortiOS traverses the configured DNS domain list to find a match. Because *host1* is mapped to the *host1.sample.com*, FortiOS resolves *host1* to *sample.com*, the first entry in the domain list.

3. Entering `ping host2`.

The system returns the following response:

```
PING host2.example.com (2.2.2.2): 56 data bytes
```

FortiOS traverses the domain list to find a match. It first queries *sample.com*, the first entry in the domain list, but does not find a match. It then queries the second entry in the domain list, *example.com*. Because *host2* is mapped to the FQDN of *host2.example.com*, FortiOS resolves *host2* to *example.com*.

DNS timeout and retry settings

The DNS timeout and retry settings can be customized using the CLI.

```
config system dns
    set timeout <integer>
    set retry <integer>
end
```

Variable	Description
timeout <integer>	The DNS query timeout interval, in seconds (1 - 10, default = 5).
retry <integer>	The number of times to retry the DNS query (0 - 5, default - 2).

FortiGate DNS server

You can create local DNS servers for your network. Depending on your requirements, you can either manually maintain your entries (primary DNS server), or use it to refer to an outside source (secondary DNS server).

A local, primary DNS server requires that you to manually add all URL and IP address combinations. Using a primary DNS server for local services can minimize inbound and outbound traffic, and access time. Making it authoritative is not recommended, because IP addresses can change, and maintaining the list can become labor intensive.

A secondary DNS server refers to an alternate source to obtain URL and IP address combinations. This is useful when there is a primary DNS server where the entry list is maintained.

FortiGate as a DNS server also supports TLS connections to a DNS client. See [DNS over TLS on page 362](#) for details.

By default, DNS server options are not available in the FortiGate GUI.

To enable DNS server options in the GUI:

1. Go to *System > Feature Visibility*.
2. Enable *DNS Database* in the *Additional Features* section.
3. Click *Apply*.

Example configuration

This section describes how to create an unauthoritative primary DNS server. The interface mode is recursive so that, if the request cannot be fulfilled, the external DNS servers will be queried.

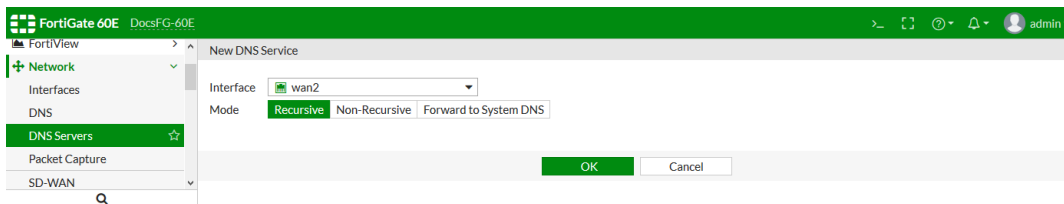
To configure FortiGate as a primary DNS server in the GUI:

1. Go to *Network > DNS Servers*.
2. In the *DNS Database* table, click *Create New*.
3. Set *Type* to *Master*.
4. Set *View* to *Shadow*.
The *View* setting controls the accessibility of the DNS server. If you select *Public*, external users can access or use the DNS server. If you select *Shadow*, only internal users can use it.
5. Enter a *DNS Zone*, for example, *WebServer*.
6. Enter the *Domain Name* of the zone, for example, *fortinet.com*.
7. Enter the *Hostname* of the DNS server, for example, *Corporate*.
8. Enter the *Contact Email Address* for the administrator, for example, *admin@example.com*.
9. Disable *Authoritative*.

10. Add DNS entries:
 - a. In the *DNS Entries* table, click *Create New*.
 - b. Select a *Type*, for example *Address (A)*.
 - c. Set the *Hostname*, for example *web.example.com*.

- d. Configure the remaining settings as needed. The options vary depending on the selected *Type*.
 - e. Click *OK*.
11. Add more DNS entries as needed.

12. Click **OK**.
13. Enable DNS services on an interface:
 - a. Go to **Network > DNS Servers**.
 - b. In the **DNS Service on Interface** table, click **Create New**.
 - c. Select the **Interface** for the DNS server, such as **wan2**.
 - d. Set the **Mode** to **Recursive**.



- e. Click **OK**.

To configure FortiGate as a primary DNS server in the CLI:

```
config system dns-database
  edit WebServer
    set domain example.com
    set type master
    set view shadow
    set ttl 86400
    set primary-name corporate
    set contact admin@example.com
    set authoritative disable
    config dns-entry
      edit 1
        set hostname web.example.com
        set type A
        set ip 192.168.21.12
        set status enable
      next
    end
  next
end

config system dns-server
  edit wan1
    set mode recursive
  next
end
```

DDNS

If your external IP address changes regularly and you want a static domain name, you can configure the external interface to use a dynamic DNS (DDNS) service. This ensures that external users and customers can always connect to your company firewall. You can configure FortiGuard as the DDNS server using the GUI or CLI.

A license or subscription is not required to use the DDNS service, but configuring DDNS in the GUI is not supported if:

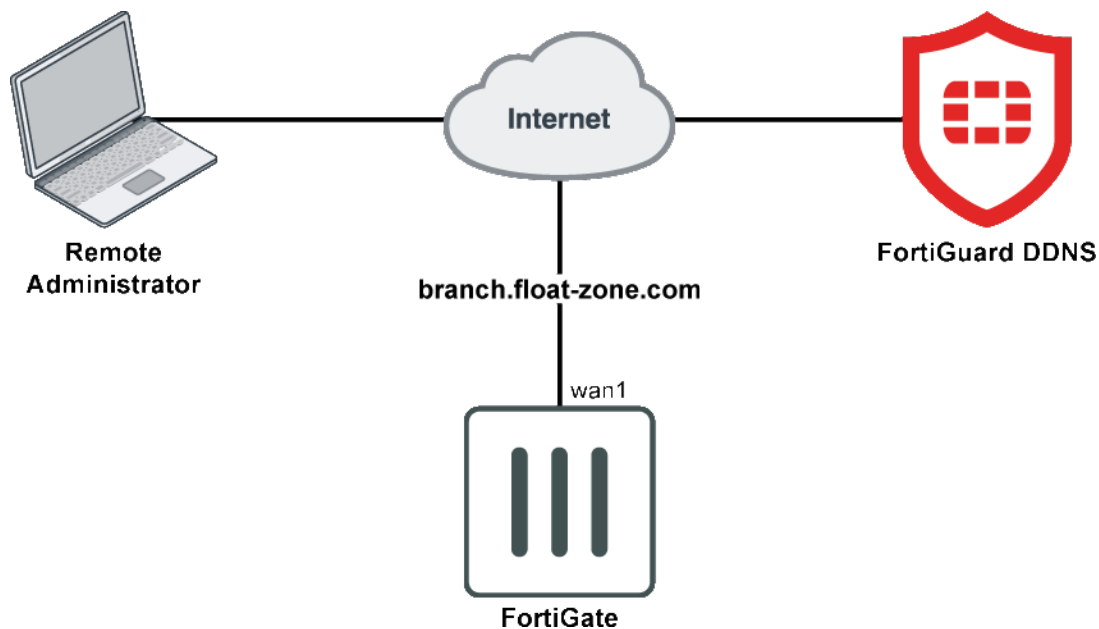
- The FortiGate model is a 1000-series or higher.
- The FortiGate is a VM.

- The DNS server is not using FortiGuard as the DNS.



FortiGate does not support DDNS when in transparent mode.

Sample topology



To configure FortiGuard as the DDNS server in the GUI:

1. Go to *Network > DNS*
2. Enable *FortiGuard DDNS*.
3. Select the *Interface* with the dynamic connection.
4. Select the *Server* that you have an account with.
5. Enter your *Unique Location*.

☒ FortiGuard DDNS

Interface	wan1
Use Public IP Address	<input type="checkbox"/>
Server	float-zone.com
Unique Location	branch
Domain	branch.float-zone.com (172.16.200.1)

6. Click *Apply*.

To configure FortiGuard as the DDNS server in the CLI:

```

config system ddns
  edit <1>
    set ddns-server FortiGuardDDNS
    set ddns-domain "branch.float-zone.com"
  
```

```
        set monitor-interface "wan1"
    next
end
```

DDNS servers other than FortiGuard

If you do not have a FortiGuard subscription, or want to use a different DDNS server, you can configure a DDNS server for each interface. Only the first configured port appears in the GUI. The available commands vary depending on the selected DDNS server.

To configure DDNS servers other than FortiGuard in the CLI:

```
config system ddns
    edit <DDNS_ID>
        set monitor-interface <external_interface>
        set ddns-server <ddns_server_selection>
        ...
    next
end
```

Refresh DDNS IP addresses

You can configure FortiGate to refresh DDNS IP addresses. FortiGate periodically checks the DDNS server that is configured.

To configure FortiGate to refresh DDNS IP addresses using the CLI:

```
config system ddns
    edit <1>
        set ddns-server FortiGuardDDNS
        set use-public-ip enable
        set update-interval seconds
    next
end
```

Disable cleartext

When `clear-text` is disabled, FortiGate uses the SSL connection to send and receive (DDNS) updates.

To disable cleartext and set the SSL certificate using the CLI:

```
config system ddns
    edit <1>
        set clear-text disable
        set ssl-certificate <cert_name>
    next
end
```

DDNS update override

A DHCP server has an override command option that allows DHCP server communications to go through DDNS to perform updates for the DHCP client. This enforces a DDNS update of the A field every time even if the DHCP client does not request it. This allows support for the `allow`, `ignore`, and `deny client-updates` options.

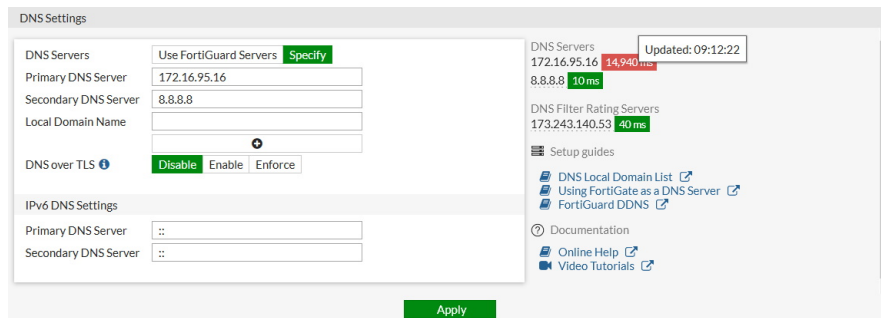
To enable DDNS update override using the CLI:

```
config system dhcp server
    edit <0>
        set ddns-update enable
        set ddns-update_override enable
        set ddns-server-ip <ddns_server_ip>
        set ddns-zone <ddns_zone>
    next
end
```

DNS latency information

High latency in DNS traffic can result in an overall sluggish experience for end-users. In the *DNS Settings* pane, you can quickly identify DNS latency issues in your configuration.

Go to *Network > DNS* to view DNS latency information in the right side bar. If you use FortiGuard DNS, latency information for DNS, DNS filter, web filter, and outbreak prevention servers is also visible. Hover your pointer over a latency value to see when it was last updated.



To view DNS latency information using the CLI:

```
# diagnose test application dnsproxy 2
worker idx: 0
worker: count=1 idx=0
retry_interval=500 query_timeout=1495
DNS latency info:
vfid=0 server=2001::1 latency=1494 updated=73311
vfid=0 server=208.91.112.52 latency=1405 updated=2547
vfid=0 server=208.91.112.53 latency=19 updated=91
SDNS latency info:
vfid=0 server=173.243.138.221 latency=1 updated=707681
DNS_CACHE: alloc=35, hit=26
RATING_CACHE: alloc=1, hit=49
DNS UDP: req=66769 res=63438 fwd=83526 alloc=0 cmp=0 retrans=16855 to=3233
         cur=111 switched=8823467 num_switched=294 v6_cur=80 v6_switched=7689041 num_v6_
switched=6
         ftg_res=8 ftg_fwd=8 ftg_retrans=0
DNS TCP: req=0, res=0, fwd=0, retrans=0 alloc=0, to=0
EQDN: alloc=45 nl_write_cnt=9498 nl_send_cnt=21606 nl_cur_cnt=0
Botnet: searched=57 hit=0 filtered=57 false_positive=0
```

To view the latency from web filter and outbreak protection servers using the CLI:

```
# diagnose debug rating
Locale    : english
```

```
Service   : Web-filter
Status    : Enable
License   : Contract
```

```
Service   : Antispam
Status    : Disable
```

```
Service   : Virus Outbreak Prevention
Status    : Disable
```

```
-- Server List (Tue Jan 22 08:03:14 2019) --
```

IP	Weight	RTT	Flags	TZ	Packets	Curr	Lost	Total	Lost	Updated	Time
173.243.138.194	10	0	DI	-8	700	0		2		Tue Jan 22 08:02:44	
2019											
173.243.138.195	10	0		-8	698	0		4		Tue Jan 22 08:02:44	
2019											
173.243.138.198	10	0		-8	698	0		4		Tue Jan 22 08:02:44	
2019											
173.243.138.196	10	0		-8	697	0		3		Tue Jan 22 08:02:44	
2019											
173.243.138.197	10	1		-8	694	0		0		Tue Jan 22 08:02:44	
2019											
96.45.33.64	10	22	D	-8	701	0		6		Tue Jan 22 08:02:44	
2019											
64.26.151.36	40	62		-5	704	0		10		Tue Jan 22 08:02:44	
2019											
64.26.151.35	40	62		-5	703	0		9		Tue Jan 22 08:02:44	
2019											
209.222.147.43	40	70	D	-5	696	0		1		Tue Jan 22 08:02:44	
2019											
66.117.56.42	40	70		-5	697	0		3		Tue Jan 22 08:02:44	
2019											
66.117.56.37	40	71		-5	702	0		9		Tue Jan 22 08:02:44	
2019											
65.210.95.239	40	74		-5	695	0		1		Tue Jan 22 08:02:44	
2019											
65.210.95.240	40	74		-5	695	0		1		Tue Jan 22 08:02:44	
2019											
45.75.200.88	90	142		0	706	0		12		Tue Jan 22 08:02:44	
2019											
45.75.200.87	90	155		0	714	0		20		Tue Jan 22 08:02:44	
2019											
45.75.200.85	90	156		0	711	0		17		Tue Jan 22 08:02:44	
2019											
45.75.200.86	90	159		0	704	0		10		Tue Jan 22 08:02:44	
2019											
62.209.40.72	100	157		1	701	0		7		Tue Jan 22 08:02:44	
2019											
62.209.40.74	100	173		1	705	0		11		Tue Jan 22 08:02:44	
2019											

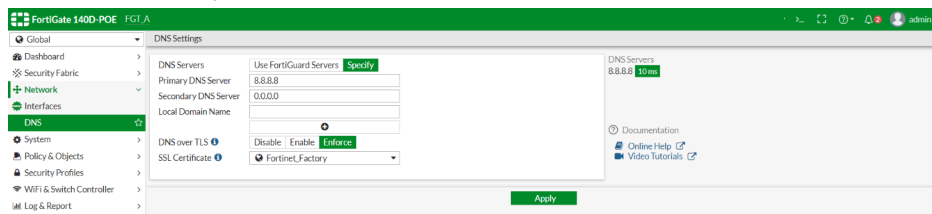
62.209.40.73	100	173	1	699	0	5	Tue Jan 22 08:02:44 2019
121.111.236.179	180	138	9	706	0	12	Tue Jan 22 08:02:44 2019
121.111.236.180	180	138	9	704	0	10	Tue Jan 22 08:02:44 2019

DNS over TLS

DNS over TLS (DoT) is a security protocol for encrypting and wrapping DNS queries and answers via the TLS protocol. The goal of DNS over TLS is to increase user privacy and security by preventing eavesdropping and manipulation of DNS data via man-in-the-middle attacks. There is an option in the FortiOS DNS profile settings to enforce DoT for this added security.

To configure DoT in the GUI:

1. Go to *Network > DNS*. The *DNS Settings* pane opens.
2. For *DNS over TLS*, click *Enforce*.



3. Click *Apply*.

To configure DoT in the CLI:

```
config system dns
    set primary 8.8.8.8
    set dns-over-tls enforce
    set ssl-certificate "Fortinet_Factory"
end
```

DNS troubleshooting

The following diagnose command can be used to collect DNS debug information. If you do not specify worker ID, the default worker ID is 0.

```
# diagnose test application dnspoxy
worker idx: 0
1. Clear DNS cache
2. Show stats
3. Dump DNS setting
4. Reload FQDN
5. Requery FQDN
6. Dump FQDN
7. Dump DNS cache
8. Dump DNS DB
9. Reload DNS DB
```


10. Dump secure DNS policy/profile
11. Dump Botnet domain
12. Reload Secure DNS setting
13. Show Hostname cache
14. Clear Hostname cache
15. Show SDNS rating cache
16. Clear SDNS rating cache
17. DNS debug bit mask
99. Restart dnsproxy worker

To view useful information about the ongoing DNS connection:

```
# diagnose test application dnsproxy 3
```

Important fields include:

tls	1 if the connection is TLS, 0 if the connection is not TLS.
rt	The round trip time of the DNS latency.
probe	The number of probes sent.

To dump the second DNS worker's cache:

```
diagnose test application dnsproxy 7 1
```

To enable debug on the second worker:

```
diagnose debug application dnsproxy -1 1
```

To enable debug on all workers by specifying -1 as worker ID:

```
diagnose debug application dnsproxy -1 -1
```

Explicit and transparent proxies

This section contains instructions for configuring explicit and transparent proxies.

- [Explicit web proxy on page 364](#)
- [Transparent proxy on page 368](#)
- [FTP proxy on page 366](#)
- [Proxy policy addresses on page 371](#)
- [Proxy policy security profiles on page 379](#)
- [Explicit proxy authentication on page 385](#)
- [Transparent web proxy forwarding on page 391](#)
- [Multiple dynamic header count on page 392](#)
- [Restricted SaaS access \(Office 365, G Suite, Dropbox\) on page 395](#)
- [Explicit proxy and FortiSandbox Cloud on page 397](#)

Explicit web proxy

Explicit web proxy can be configured on FortiGate for proxying HTTP and HTTPS traffic.

To deploy explicit proxy, individual client browsers can be manually configured to send requests directly to the proxy, or they can be configured to download proxy configuration instructions from a Proxy Auto-Configuration (PAC) file.

When explicit proxy is configured on an interface, the interface IP address can be used by client browsers to forward requests directly to the FortiGate. FortiGate also supports PAC file configuration.

To configure explicit web proxy in the GUI:

1. Enable and configure explicit web proxy:
 - a. Go to *Network > Explicit Proxy*.
 - b. Enable *Explicit Web Proxy*.
 - c. Select *port2* as the *Listen on Interfaces* and set the *HTTP Port* to *8080*.
 - d. Configure the remaining settings as needed.

- e. Click *Apply*.
2. Create an explicit web proxy policy:
 - a. Go to *Policy & Objects > Proxy Policy*.
 - b. Click *Create New*.
 - c. Set *Proxy Type* to *Explicit Web* and *Outgoing Interface* to *port1*.

- d. Also set *Source* and *Destination* to *all*, *Schedule* to *always*, *Service* to *webproxy*, and *Action* to *ACCEPT*.

- e. Click OK to create the policy.



This example creates a basic policy. If required, security profiles can be enabled, and deep SSL inspection can be selected to inspect HTTPS traffic.

3. Configure a client to use the FortiGate explicit proxy:

Set the FortiGate IP address as the proxy IP address in the browser, or use an automatic configuration script for the PAC file.

To configure explicit web proxy in the CLI:

1. Enable and configure explicit web proxy:

```
config web-proxy explicit
  set status enable
  set ftp-over-http enable
  set socks enable
  set http-incoming-port 8080
  set ipv6-status enable
  set unknown-http-version best-effort
end
config system interface
```

```
edit "port2"
    set vdom "vdom1"
    set ip 10.1.100.1 255.255.255.0
    set allowaccess ping https ssh snmp http telnet
    set type physical
    set explicit-web-proxy enable
    set snmp-index 12
end
next
end
```

2. Create an explicit web proxy policy:

```
config firewall proxy-policy
    edit 1
        set uuid 722b6130-13aa-51e9-195b-c4196568d667
        set proxy explicit-web
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set service "webproxy"
        set action accept
        set schedule "always"
        set logtraffic all
    next
end
```



This example creates a basic policy. If required, security profiles can be enabled, and deep SSL inspection can be selected to inspect HTTPS traffic.

3. Configure a client to use the FortiGate explicit web proxy:

Set the FortiGate IP address as the proxy IP address in the browser, or use an automatic configuration script for the PAC file.

FTP proxy

FTP proxies can be configured on the FortiGate so that FTP traffic can be proxied. When the FortiGate is configured as an FTP proxy, FTP client applications should be configured to send FTP requests to the FortiGate.

To configure explicit FTP proxy in the GUI:

1. Enable and configure explicit FTP proxy:
 - a. Go to *Network > Explicit Proxy*.
 - b. Enable *Explicit FTP Proxy*.
 - c. Select *port2* as the *Listen on Interfaces* and set the *HTTP Port* to *21*.

- d. Configure the *Default Firewall Policy Action* as needed.

- e. Click *Apply*.

2. Create an explicit FTP proxy policy:

- a. Go to *Policy & Objects > Proxy Policy*.
- b. Click *Create New*.
- c. Set *Proxy Type* to *FTP* and *Outgoing Interface* to *port1*.
- d. Also set *Source* and *Destination* to *all*, *Schedule* to *always*, and *Action* to *ACCEPT*.

- e. Click *OK* to create the policy.



This example creates a basic policy. If required, security profiles can be enabled.

3. Configure the FTP client application to use the FortiGate IP address.

To configure explicit FTP proxy in the CLI:

1. Enable and configure explicit FTP proxy:

```
config ftp-proxy explicit
    set status enable
    set incoming-port 21
end
config system interface
    edit "port2"
        set vdom "vdom1"
        set ip 10.1.100.1 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
        set type physical
        set explicit-ftp-proxy enable
        set snmp-index 12
    end
next
end
```

2. Create an explicit FTP proxy policy:

```
config firewall proxy-policy
    edit 4
        set uuid 2e945a3a-565d-51e9-4fac-5215d287adc0
        set proxy ftp
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
    next
end
```



This example creates a basic policy. If required, security profiles can be enabled.

3. Configure the FTP client application to use the FortiGate IP address.

Transparent proxy

In a transparent proxy deployment, the user's client software, such as a browser, is unaware that it is communicating with a proxy.

Users request Internet content as usual, without any special client configuration, and the proxy serves their requests. FortiGate also allows user to configure in transparent proxy mode.

To configure transparent proxy in the GUI:

1. Configure a regular firewall policy with HTTP redirect:

- a. Go to *Policy & Objects > IPv4 Policy*.
- b. Click *Create New*.
- c. Name the policy appropriately, set the *Incoming Interface* to *port2*, and set the *Outgoing Interface* to *port1*.

- d. Also set *Source* and *Destination* to *all*, *Schedule* to *always*, *Service* to *ALL*, and *Action* to *ACCEPT*.
- e. Set *Inspection Mode* to *Proxy-based* and *SSL Inspection* to *deep-inspection*.

The screenshot shows the 'New Policy' configuration window in the FortiGate GUI. The policy is named 'LAN To WAN'. The Incoming Interface is 'port2' and the Outgoing Interface is 'port1'. Source and Destination are both set to 'all'. The Schedule is 'always' and the Service is 'ALL'. The Action is 'ACCEPT'. The Inspection Mode is 'Proxy-based'. The Firewall / Network Options section shows NAT is disabled and Protocol Options are set to 'default'. The Security Profiles section shows AntiVirus and Web Filter are disabled. The OK button is highlighted in green.

- f. Configure the remaining settings as needed.
- g. Click **OK**.



By default, HTTP redirect can only be enabled in the CLI. Enable *Policy Advanced Options* in *Feature Visibility* to configure it in the GUI. See [Feature visibility on page 732](#) on page 1 for more information.

To redirect HTTPS traffic, SSL inspection is required.

2. Configure a transparent proxy policy:
 - a. Go to *Policy & Objects > Proxy Policy*.
 - b. Click *Create New*.
 - c. Set *Proxy Type* to *Transparent Web*, set the *Incoming Interface* to *port2*, and set the *Outgoing Interface* to *port1*.

- d. Also set *Source* and *Destination* to *all*, *Schedule* to *always*, *Service* to *webproxy*, and *Action* to *ACCEPT*.

- e. Configure the remaining settings as needed.
f. Click **OK** to create the policy.



This example creates a basic policy. If required, security profiles can be enabled, and deep SSL inspection can be selected to inspect HTTPS traffic.

3. No special configure is required on the client to use FortiGate transparent proxy. As the client is using the FortiGate as its default gateway, requests will first hit the regular firewall policy, and then be redirected to the transparent proxy policy.

To configure transparent proxy in the CLI:

1. Configure a regular firewall policy with HTTP redirect:

```
config firewall policy
  edit 1
    set name "1"
    set srcintf "port2"
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set inspection-mode proxy
    set http-policy-redirect enable
    set fsso disable
    set ssl-ssh-profile "deep-inspection"
    set nat enable
  next
end
```


2. Configure a transparent proxy policy:

```
config firewall proxy-policy
  edit 5
    set proxy transparent-web
    set srcintf "port2"
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "all"
    set service "webproxy"
    set action accept
    set schedule "always"
  next
end
```



This example creates a basic policy. If required, security profiles can be enabled, and deep SSL inspection can be selected to inspect HTTPS traffic.

3. No special configure is required on the client to use FortiGate transparent proxy. As the client is using the FortiGate as its default gateway, requests will first hit the regular firewall policy, and then be redirected to the transparent proxy policy.

Proxy policy addresses

Proxy addresses are designed to be used only by proxy policies. The following address types are available:

- [Host regex match on page 372](#)
- [URL pattern on page 372](#)
- [URL category on page 373](#)
- [HTTP method on page 374](#)
- [HTTP header on page 375](#)
- [User agent on page 376](#)
- [Advanced \(source\) on page 377](#)
- [Advanced \(destination\) on page 378](#)

Fast policy match

The fast policy match function improves the performance of IPv4 explicit and transparent web proxies on FortiGate devices.

When enabled, after the proxy policies are configured, the FortiGate builds a fast searching table based on the different proxy policy matching criteria. When fast policy matching is disabled, web proxy traffic is compared to the policies one at a time from the beginning of the policy list.

Fast policy matching is enabled by default, and can be configured with the following CLI command:

```
config web-proxy global
  set fast-policy-match {enable | disable}
end
```

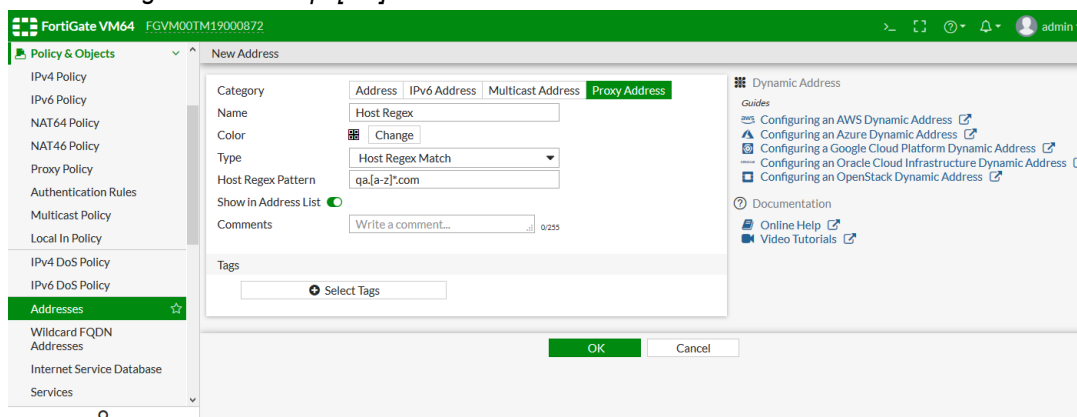
Host regex match

In this address type, a user can create a hostname as a regular expression. Once created, the hostname address can be selected as a destination of a proxy policy. This means that a policy will only allow or block requests that match the regular expression.

This example creates a host regex match address with the pattern `qa.[a-z]*.com`.

To create a host regex match address in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address*.
3. Set the following:
 - *Category* to *Proxy Address*,
 - *Name* to *Host Regex*,
 - *Type* to *Host Regex Match*, and
 - *Host Regex Pattern* to `qa.[a-z]*.com`.



4. Click *OK*.

To create a host regex match address in the CLI:

```
config firewall proxy-address
edit "Host Regex"
set uuid 8e374390-57c9-51e9-9353-ee4469629df8
set type host-regex
set host-regex "qa.[a-z]*.com"
next
end
```

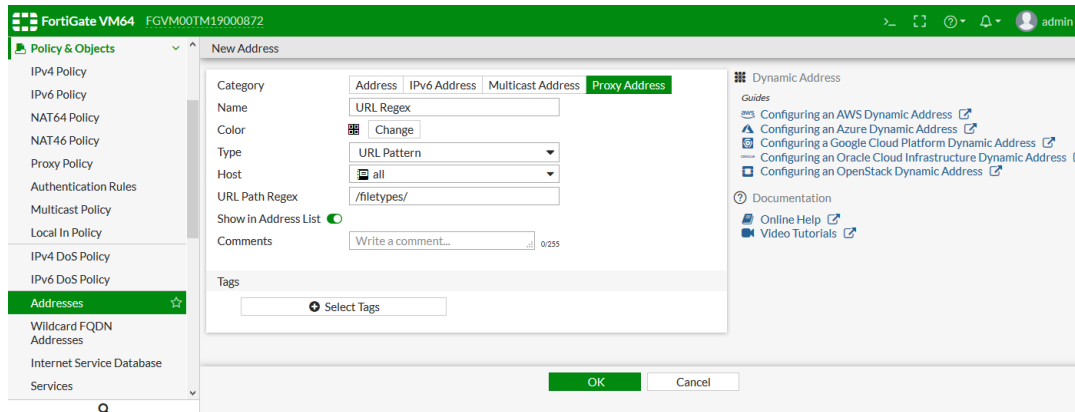
URL pattern

In this address type, a user can create a URL path as a regular expression. Once created, the path address can be selected as a destination of a proxy policy. This means that a policy will only allow or block requests that match the regular expression.

This example creates a URL pattern address with the pattern `/filetypes/`.

To create a URL pattern address in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address*.
3. Set the following:
 - *Category* to *Proxy Address*,
 - *Name* to *URL Regex*,
 - *Type* to *URL Pattern*,
 - *Host* to *all*, and
 - *URL Path Regex* to */filetypes/*.



4. Click **OK**.

To create a URL pattern address in the CLI:

```
config firewall proxy-address
  edit "URL Regex"
    set uuid 267dc8e4-57cb-51e9-0cfe-27877bfff51d3
    set type url
    set host "all"
    set path "/filetypes/"
  next
end
```

URL category

In this address type, a user can create a URL category based on a FortiGuard URL ID. Once created, the address can be selected as a destination of a proxy policy. This means that a policy will only allow or block requests that match the URL category.

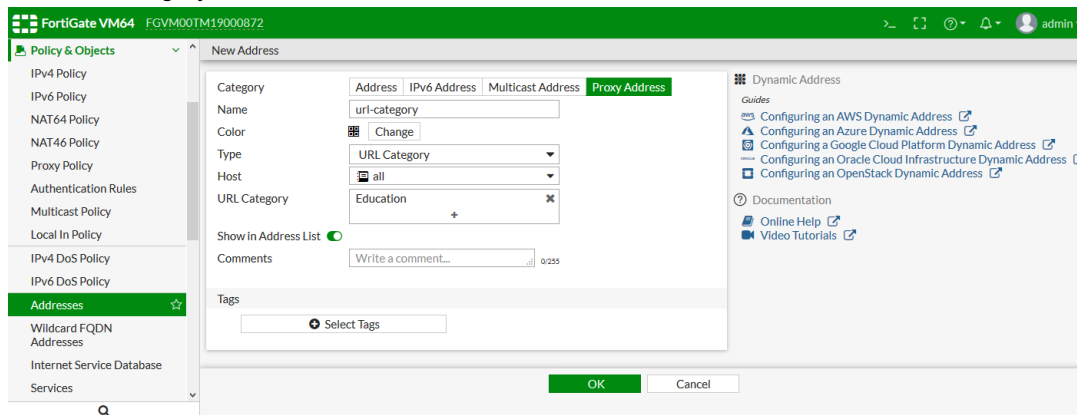
The example creates a URL category address for URLs in the *Education* category. For more information about categories, see <https://fortiguard.com/webfilter/categories>.

To create a URL category address in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address*.

3. Set the following:

- *Category* to *Proxy Address*,
- *Name* to *url-category*,
- *Type* to *URL Category*,
- *Host* to *all*, and
- *URL Category* to *Education*.



4. Click OK.

To create a URL category address in the CLI:

```
config firewall proxy-address
  edit "url-category"
    set uuid 7a5465d2-57cf-51e9-49fd-0c6b5ad2ff4f
    set type category
    set host "all"
    set category 30
  next
end
```

To see a list of all the categories and their numbers, when editing the address, enter `set category ?`.

HTTP method

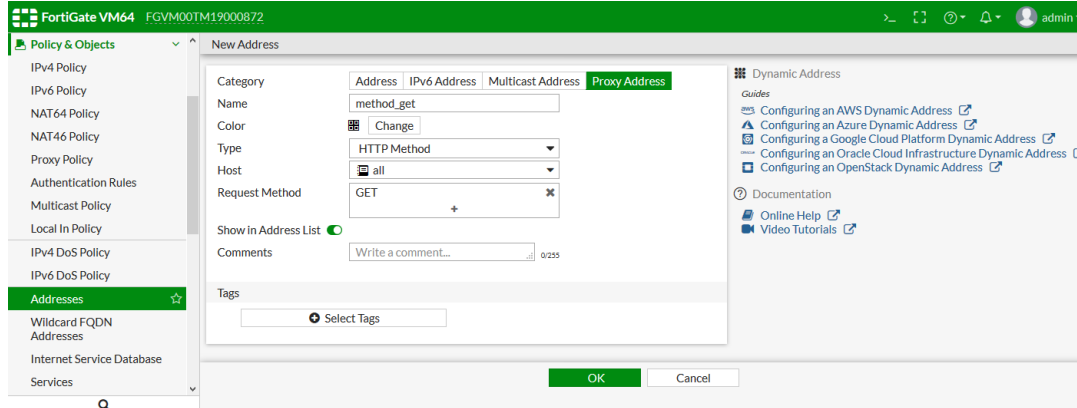
In this address type, a user can create an address based on the HTTP request methods that are used. Multiple method options are supported, including: *CONNECT*, *DELETE*, *GET*, *HEAD*, *OPTIONS*, *POST*, *PUT*, and *TRACE*. Once created, the address can be selected as a source of a proxy policy. This means that a policy will only allow or block requests that match the selected HTTP method.

The example creates a HTTP method address that uses the GET method.

To create a HTTP method address in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address*.
3. Set the following:
 - *Category* to *Proxy Address*,
 - *Name* to *method_get*,
 - *Type* to *HTTP Method*,

- *Host to all*, and
- *Request Method to GET*.



4. Click **OK**.

To create a HTTP method address in the CLI:

```
config firewall proxy-address
  edit "method_get"
    set uuid 1e4d1a02-57d6-51e9-a5c4-73387925b7de
    set type method
    set host "all"
    set method get
  next
end
```

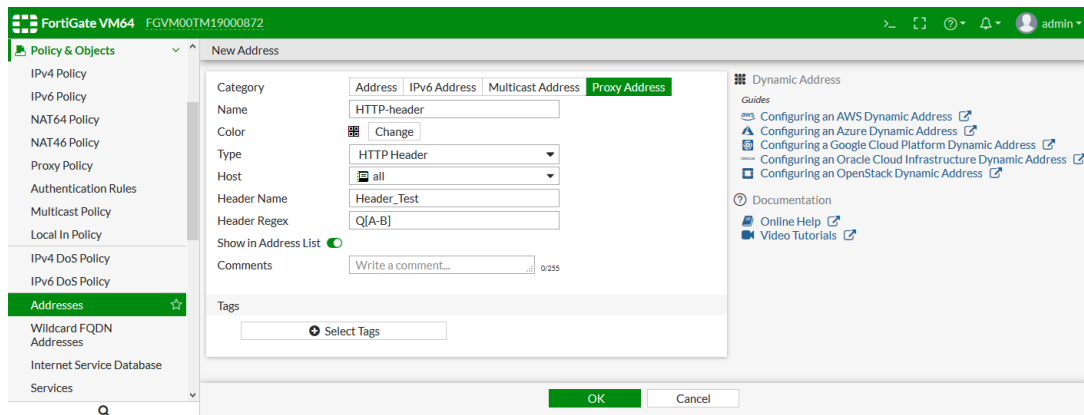
HTTP header

In this address type, a user can create a HTTP header as a regular expression. Once created, the header address can be selected as a source of a proxy policy. This means that a policy will only allow or block requests where the HTTP header matches the regular expression.

This example creates a HTTP header address with the pattern *Q[A-B]*.

To create a HTTP header address in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address*.
3. Set the following:
 - *Category to Proxy Address*,
 - *Name to HTTP-header*,
 - *Type to HTTP Header*,
 - *Host to all*,
 - *Header Name to Header_Test*, and
 - *Header Regex to Q[A-B]*.



4. Click OK.

To create a HTTP header address in the CLI:

```
config firewall proxy-address
  edit "method_get"
    set uuid a0f1b806-57e9-51e9-b214-7a1cfafa9bb3
    set type header
    set host "all"
    set header-name "Header_Test"
    set header "Q[A-B]"
  next
end
```

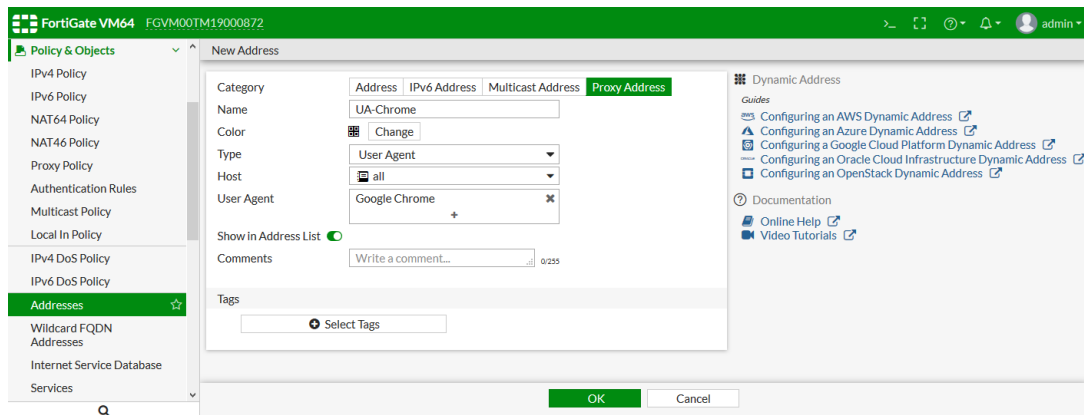
User agent

In this address type, a user can create an address based on the names of the browsers that are used as user agents. Multiple browsers are supported, such as Chrome, Firefox, Internet Explorer, and others. Once created, the address can be selected as a source of a proxy policy. This means that a policy will only allow or block requests from the specified user agent.

This example creates a user agent address for Google Chrome.

To create a user agent address in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address*.
3. Set the following:
 - *Category* to *Proxy Address*,
 - *Name* to *UA-Chrome*,
 - *Type* to *User Agent*,
 - *Host* to *all*, and
 - *User Agent* to *Google Chrome*.



4. Click **OK**.

To create a user agent address in the CLI:

```
config firewall proxy-address
  edit "UA-Chrome"
    set uuid e3550196-57d8-51e9-eed0-115095a7920b
    set type ua
    set host "all"
    set ua chrome
  next
end
```

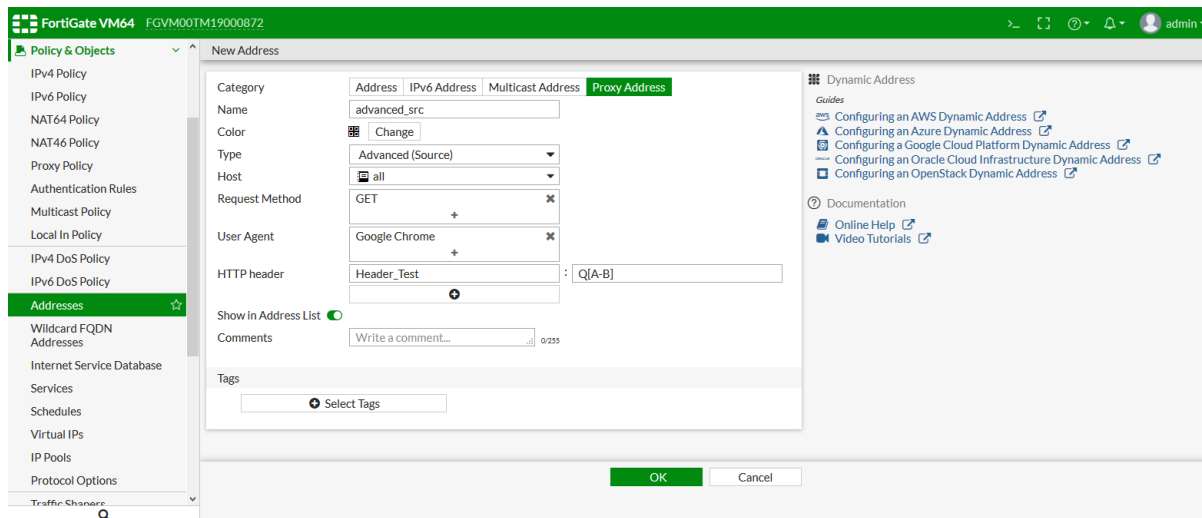
Advanced (source)

In this address type, a user can create an address based on multiple parameters, including HTTP method, User Agent, and HTTP header. Once created, the address can be selected as a source of a proxy policy. This means that a policy will only allow or block requests that match the selected address.

This example creates an address that uses the get method, a user agent for Google Chrome, and an HTTP header with the pattern `Q[A-B]`.

To create an advanced (source) address in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address*.
3. Set the following:
 - *Category* to *Proxy Address*,
 - *Name* to *advanced_src*,
 - *Type* to *Advanced (Source)*,
 - *Host* to *all*,
 - *Request Method* to *GET*,
 - *User Agent* to *Google Chrome*, and
 - *HTTP header* to *Header_Test : Q[A-B]*.



4. Click OK.

To create an advanced (source) address in the CLI:

```
config firewall proxy-address
  edit "advance_src"
    set uuid fb9991d0-57e3-51e9-9fed-855e0bca16c3
    set type src-advanced
    set host "all"
    set method get
    set ua chrome
    config header-group
      edit 1
        set header-name "Header_Test"
        set header "Q[A-B]"
      next
    end
  next
end
```

Advanced (destination)

In this address type, a user can create an address based on URL pattern and URL category parameters. Once created, the address can be selected as a destination of a proxy policy. This means that a policy will only allow or block requests that match the selected address.

This example creates an address with the URL pattern */about* that are in the *Education* category. For more information about categories, see <https://fortiguard.com/webfilter/categories>.

To create an advanced (destination) address in the GUI:

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address*.
3. Set the following:
 - *Category* to *Proxy Address*,
 - *Name* to *Advanced-dst*,

- *Type to Advanced (Destination),*
- *Host to all,*
- *URL Path Regex to /about, and*
- *URL Category to Education.*

4. Click OK.

To create an advanced (destination) address in the CLI:

```
config firewall proxy-address
  edit "Advanced-dst"
    set uuid d9c2a0d6-57e5-51e9-8c92-6aa8b3372198
    set type dst-advanced
    set host "ubc"
    set path "/about"
    set category 30
  next
end
```

Proxy policy security profiles

Web proxy policies support most security profile types.



Security profiles must be created before they can be used in a policy, see [Security Profiles on page 907](#) for information.

Explicit web proxy policy

The security profiles supported by explicit web proxy policies are:

- *AntiVirus*
- *Web Filter*
- *Application Control*
- *IPS*
- *DLP Sensor*

- *ICAP*
- *Web Application Firewall*
- *SSL Inspection*

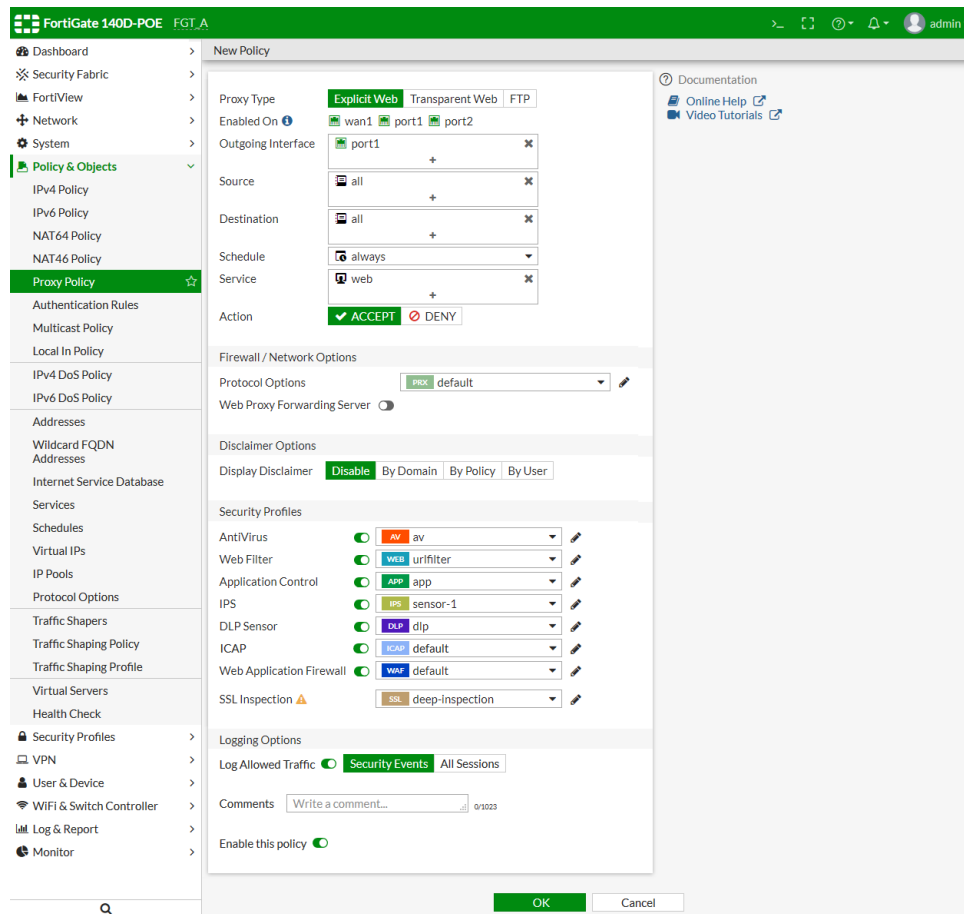
To configure security profiles on an explicit web proxy policy in the GUI:

1. Go to *Policy & Objects > Proxy Policy*.
2. Click *Create New*.
3. Set the following:

Proxy Type	Explicit Web
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	webproxy
Action	ACCEPT

4. In the *Firewall / Network Options* section, set *Protocol Options* to *default*.
5. In the *Security Profiles* section, make the following selections (for this example, these profiles have all already been created):

AntiVirus	av
Web Filter	urlfiler
Application Control	app
IPS	Sensor-1
DLP Sensor	dlp
ICAP	default
Web Application Firewall	default
SSL Inspection	deep-inspection



6. Click OK to create the policy.

To configure security profiles on an explicit web proxy policy in the CLI:

```
config firewall proxy-policy
  edit 1
    set uuid c8a71a2c-54be-51e9-fa7a-858f83139c70
    set proxy explicit-web
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "all"
    set service "web"
    set action accept
    set schedule "always"
    set utm-status enable
    set av-profile "av"
    set webfilter-profile "urlfilter"
    set dlp-sensor "dlp"
    set ips-sensor "sensor-1"
    set application-list "app"
    set icap-profile "default"
    set waf-profile "default"
    set ssl-ssh-profile "deep-inspection"
  next
end
```

Transparent proxy

The security profiles supported by transparent proxy policies are:

- *AntiVirus*
- *Web Filter*
- *Application Control*
- *IPS*
- *DLP Sensor*
- *ICAP*
- *Web Application Firewall*
- *SSL Inspection*

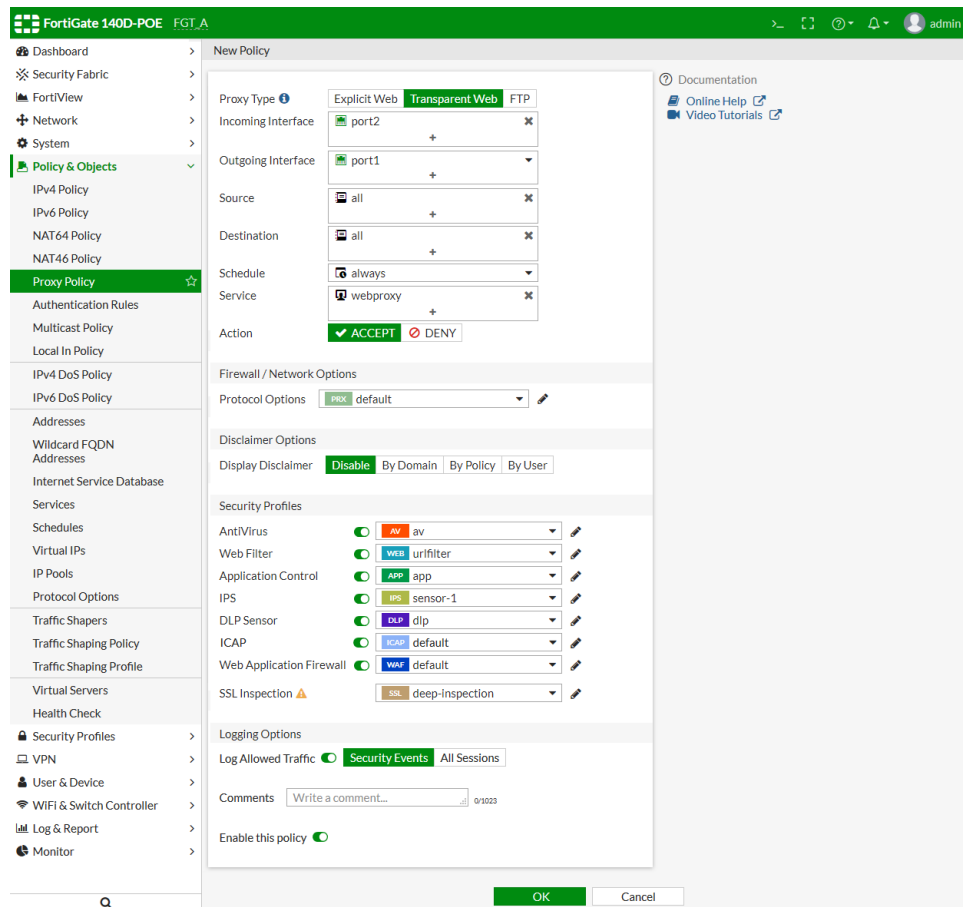
To configure security profiles on a transparent proxy policy in the GUI:

1. Go to *Policy & Objects > Proxy Policy*.
2. Click *Create New*.
3. Set the following:

Proxy Type	Transparent Web
Incoming Interface	port2
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	webproxy
Action	ACCEPT

4. In the *Firewall / Network Options* section, set *Protocol Options* to *default*.
5. In the *Security Profiles* section, make the following selections (for this example, these profiles have all already been created):

AntiVirus	av
Web Filter	urlfilter
Application Control	app
IPS	Sensor-1
DLP Sensor	dlp
ICAP	default
Web Application Firewall	default
SSL Inspection	deep-inspection



6. Click OK to create the policy.

To configure security profiles on a transparent proxy policy in the CLI:

```
config firewall proxy-policy
edit 2
set uuid 8fb05036-56fc-51e9-76a1-86f757d3d8dc
set proxy transparent-web
set srcintf "port2"
set dstintf "port1"
set srcaddr "all"
set dstaddr "all"
set service "webproxy"
set action accept
set schedule "always"
set utm-status enable
set av-profile "av"
set webfilter-profile "urlfilter"
set dlp-sensor "dlp"
set ips-sensor "sensor-1"
set application-list "app"
set icap-profile "default"
set waf-profile "default"
set ssl-ssh-profile "certificate-inspection"
```

```
next
end
```

FTP proxy

The security profiles supported by FTP proxy policies are:

- *AntiVirus*
- *Application Control*
- *IPS*
- *DLP Sensor*

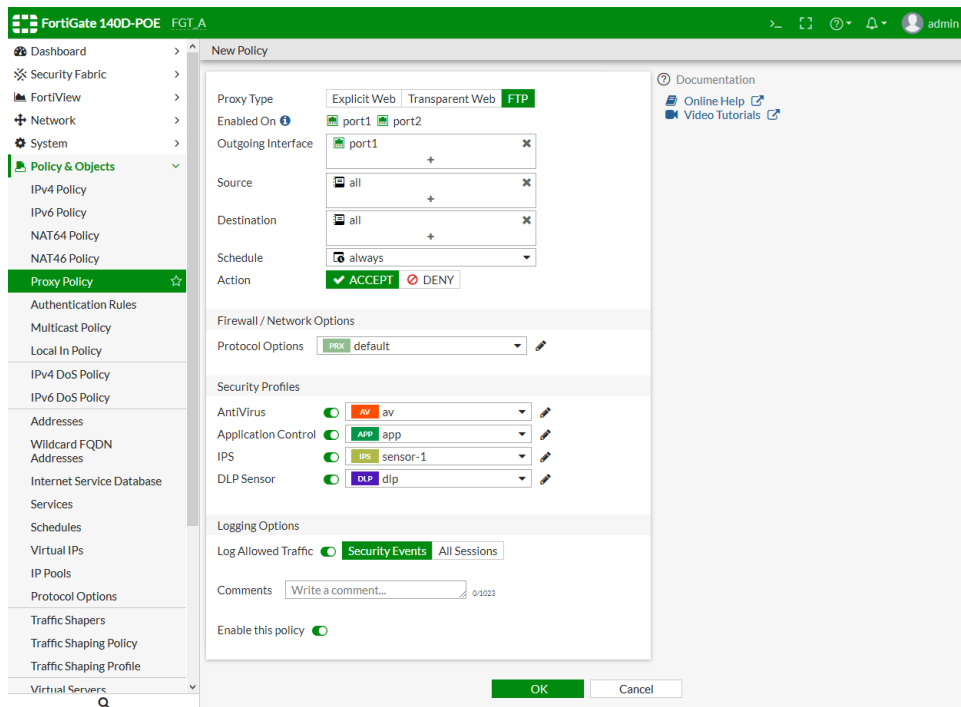
To configure security profiles on an FTP proxy policy in the GUI:

1. Go to *Policy & Objects > Proxy Policy*.
2. Click *Create New*.
3. Set the following:

Proxy Type	FTP
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Action	ACCEPT

4. In the *Firewall / Network Options* section, set *Protocol Options* to *default*.
5. In the *Security Profiles* section, make the following selections (for this example, these profiles have all already been created):

AntiVirus	av
Application Control	app
IPS	Sensor-1
DLP Sensor	dlp



6. Click **OK** to create the policy.

To configure security profiles on an FTP proxy policy in the CLI:

```
config firewall proxy-policy
  edit 3
    set uuid cb89af34-54be-51e9-4496-c69ccfc4d5d4
    set proxy ftp
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set utm-status enable
    set av-profile "av"
    set dlp-sensor "dlp"
    set ips-sensor "sensor-1"
    set application-list "app"
  next
end
```

Explicit proxy authentication

FortiGate supports multiple authentication methods. This topic explains using an external authentication server with Kerberos as the primary and NTLM as the fallback.

To configure Explicit Proxy with authentication:

1. [Enable and configure the explicit proxy on page 386.](#)
2. [Configure the authentication server and create user groups on page 386.](#)

3. [Create an authentication scheme and rules on page 388.](#)
4. [Create an explicit proxy policy and assign a user group to the policy on page 389.](#)
5. [Verify the configuration on page 390.](#)

Enable and configure the explicit proxy

To enable and configure explicit web proxy in the GUI:

1. Go to *Network > Explicit Proxy*.
2. Enable *Explicit Web Proxy*.
3. Select *port2* as the *Listen on Interfaces* and set the *HTTP Port* to *8080*.
4. Configure the remaining settings as needed.
5. Click *Apply*.

To enable and configure explicit web proxy in the CLI:

```
config web-proxy explicit
    set status enable
    set ftp-over-http enable
    set socks enable
    set http-incoming-port 8080
    set ipv6-status enable
    set unknown-http-version best-effort
end
config system interface
    edit "port2"
        set vdom "vdom1"
        set ip 10.1.100.1 255.255.255.0
        set allowaccess ping https ssh snmp http telnet
        set type physical
        set explicit-web-proxy enable
        set snmp-index 12
    end
next
end
```

Configure the authentication server and create user groups

Since we are using an external authentication server with Kerberos authentication as the primary and NTLM as the fallback, Kerberos authentication is configured first and then FSSO NTLM authentication is configured.

For successful authorization, the FortiGate checks if user belongs to one of the groups that is permitted in the security policy.

To configure an authentication server and create user groups in the GUI:

1. Configure Kerberos authentication:
 - a. Go to *User & Device > LDAP Servers*.
 - b. Click *Create New*.

- c. Set the following:

Name	ldap-kerberos
Server IP	172.18.62.220
Server Port	389
Common Name Identifier	cn
Distinguished Name	dc=fortinetqa,dc=local

- d. Click OK

2. Define Kerberos as an authentication service. This option is only available in the CLI. For information on generating a keytab, see [Generating a keytab on a Windows server on page 390](#).
3. Configure FSSO NTLM authentication:

FSSO NTLM authentication is supported in a Windows AD network. FSSO can also provide NTLM authentication service to the FortiGate unit. When a user makes a request that requires authentication, the FortiGate initiates NTLM negotiation with the client browser, but does not process the NTLM packets itself. Instead, it forwards all the NTLM packets to the FSSO service for processing.

 - a. Go to *Security Fabric > Fabric Connectors*.
 - b. Click *Create New* and select *Fortinet Single Sign-On Agent* from the *SSO/Identity* category.
 - c. Set the *Name* to *FSSO, Primary FSSO Agent* to *172.16.200.220*, and enter a password.
 - d. Click OK.
4. Create a user group for Kerberos authentication:
 - a. Go to *User & Device > User Groups*.
 - b. Click *Create New*.
 - c. Set the *Name* to *Ldap-Group*, and *Type* to *Firewall*.
 - d. In the *Remote Groups* table, click *Add*, and set the *Remote Server* to the previously created *ldap-kerberos* server.
 - e. Click OK.
5. Create a user group for NTLM authentication:
 - a. Go to *User & Device > User Groups*.
 - b. Click *Create New*.
 - c. Set the *Name* to *NTLM-FSSO-Group*, *Type* to *Fortinet Single Sign-On (FSSO)*, and add *FORTINETQA/FSSO* as a member.
 - d. Click OK.

To configure an authentication server and create user groups in the CLI:

1. Configure Kerberos authentication:

```
config user ldap
    edit "ldap-kerberos"
        set server "172.18.62.220"
        set cnid "cn"
        set dn "dc=fortinetqa,dc=local"
        set type regular
        set username "CN=root,CN=Users,DC=fortinetqa,DC=local"
        set password *****
    next
end
```

2. Define Kerberos as an authentication service:

```

config user krb-keytab
  edit "http_service"
    set pac-data disable
    set principal "HTTP/FGT.FORTINETQA.LOCAL@FORTINETQA.LOCAL"
    set ldap-server "ldap-kerberos"
    set keytab
      "BQIAABFAAIAEEZPULRJTkVUUUEuTE9DQUwABehUVFAAFEZHVC5GT1JUSU5FVFFBLkxPQ0FMAAAAAQAAAA
      EAAEACKLCMonpitnVAAAARQACABGT1JUSU5FVFFBLkxPQ0FMAARIVFRQABRGR1QuRk9SVElORVRRQS5MT0N
      BTAIAAAEAAAAABAADAAiiwJKJ6YrZ1QAAAE0AAgAQRk9SVElORVRRQS5MT0NBTAESFRUUAURkdULkZPULR
      JTkVUUUEuTE9DQUwAAAABAAAAAAQAFwAUHo9uqR9cSkzyxdzKCEXdwAAAF0AAgAQRk9SVElORVRRQS5MT0N
      BTAESFRUUAURkdULkZPULRJTkVUUUEuTE9DQUwAAAABAAAAAAQAEgAgzee854Aq1HhQiKJZvV4tL2Poy7h
      MIARQpK8MCB//BIAAAABNAAIAEEZPULRJTkVUUUEuTE9DQUwABehUVFAAFEZHVC5GT1JUSU5FVFFBLkxPQ0F
      MAAAAQAAAAEABEAEG49vHEiiBghr63Z/lnwYrU="
    next
  end

```

For information on generating a keytab, see [Generating a keytab on a Windows server on page 390](#).

3. Configure FSSO NTLM authentication:

```

config user fsso
  edit "1"
    set server "172.18.62.220"
    set password
  next
end

```

4. Create a user group for Kerberos authentication:

```

config user group
  edit "Ldap-Group"
    set member "ldap" "ldap-kerberos"
  next
end

```

5. Create a user group for NTLM authentication:

```

config user group
  edit "NTLM-FSSO-Group"
    set group-type fsso-service
    set member "FORTINETQA/FSSO"
  next
end

```

Create an authentication scheme and rules

Explicit proxy authentication is managed by authentication schemes and rules. An authentication scheme must be created first, and then the authentication rule.

To create an authentication scheme and rules in the GUI:

1. Create an authentication scheme:
 - a. Go to *Policy & Objects > Authentication Rules*.
 - b. Click *Create New > Authentication Schemes*.

- c. Set the *Name* to *Auth-scheme-Negotiate* and select *Negotiate* as the *Method*.
- d. Click OK.
2. Create an authentication rule:
 - a. Go to *Policy & Objects > Authentication Rules*.
 - b. Click *Create New > Authentication Rules*.
 - c. Set the *Name* to *Auth-Rule*, *Source Address* to *all*, and *Protocol* to *HTTP*.
 - d. Enable *Authentication Scheme*, and select the just created *Auth-scheme-Negotiate* scheme.
 - e. Click OK.

To create an authentication scheme and rules in the CLI:

1. Create an authentication scheme:

```
config authentication scheme
  edit "Auth-scheme-Negotiate"
    set method negotiate      <<< Accepts both Kerberos and NTLM as fallback
  next
end
```

2. Create an authentication rule:

```
config authentication rule
  edit "Auth-Rule"
    set status enable
    set protocol http
    set srcaddr "all"
    set ip-based enable
    set active-auth-method "Auth-scheme-Negotiate"
    set comments "Testing"
  next
end
```

Create an explicit proxy policy and assign a user group to the policy

To create an explicit proxy policy and assign a user group to it in the GUI:

1. Go to *Policy & Object > Proxy Policy*.
2. Click *Create New*.
3. Set *Proxy Type* to *Explicit Web* and *Outgoing Interface* to *port1*.
4. Set *Source* to *all*, and the just created user groups *NTLM-FSSO-Group* and *Ldap-Group*.
5. Also set *Destination* to *all*, *Schedule* to *always*, *Service* to *webproxy*, and *Action* to *ACCEPT*.
6. Click OK.

To create an explicit proxy policy and assign a user group to it in the CLI:

```
config firewall proxy-policy
  edit 1
    set uuid 722b6130-13aa-51e9-195b-c4196568d667
    set proxy explicit-web
    set dstintf "port1"
    set srcaddr "all"
    set dstaddr "all"
```

```
        set service "web"
        set action accept
        set schedule "always"
        set logtraffic all
        set groups "NTLM-FSSO-Group" "Ldap-Group"
        set av-profile "av"
        set ssl-ssh-profile "deep-custom"
    next
end
```

Verify the configuration

Log in using a domain and system that would be authenticated using the Kerberos server, then enter the `diagnose wad user list` CLI command to verify:

```
# diagnose wad user list
ID: 8, IP: 10.1.100.71, VDOM: vdom1
  user name   : test1@FORTINETQA.LOCAL
  duration    : 389
  auth_type   : IP
  auth_method : Negotiate
  pol_id      : 1
  g_id        : 1
  user_based  : 0
  expire      : no
LAN:
  bytes_in=4862 bytes_out=11893
WAN:
  bytes_in=7844 bytes_out=1023
```

Log in using a system that is not part of the domain. The NTLM fallback server should be used:

```
# diagnose wad user list
ID: 2, IP: 10.1.100.202, VDOM: vdom1
  user name   : TEST31@FORTINETQA
  duration    : 7
  auth_type   : IP
  auth_method : NTLM
  pol_id      : 1
  g_id        : 5
  user_based  : 0
  expire      : no
LAN:
  bytes_in=6156 bytes_out=16149
WAN:
  bytes_in=7618 bytes_out=1917
```

Generating a keytab on a Windows server

A keytab is used to allow services that are not running Windows to be configured with service instance accounts in the Active Directory Domain Service (AD DS). This allows Kerberos clients to authenticate to the service through Windows Key Distribution Centers (KDCs).

For an explanation of the process, see <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ktpass>.

To generate a keytab on a Windows server:

1. On the server, create a user for the FortiGate:
 - The service name is the FQDN for the explicit proxy interface, such as the hostname in the client browser proxy configuration. In this example, the service name is *FGT*.
 - The account only requires *domain users* membership.
 - The password must be very strong.
 - The password is set to never expire.
2. Add the FortiGate FQDN in to the Windows DNS domain, as well as in-addr.arpa.
3. Generate the Kerberos keytab using the `ktpass` command on Windows servers and many domain workstations:

```
# ktpass -princ HTTP/<domain name of test fgt>@realm -mapuser <user> -pass <password> -crypto all -ptype KRB5_NT_PRINCIPAL -out fgt.keytab
```

For example:

```
ktpass -princ HTTP/FGT.FORTINETQA.LOCAL@FORTINETQA.LOCAL -mapuser FGT -pass ***** -crypto all -ptype KRB5_NT_PRINCIPAL -out fgt.keytab
```



If the FortiGate is handling multiple keytabs in Kerberos authentication, use different passwords when generating each keytab.

4. Encode the keytab to base64 in a text file:
 - On Windows: `certutil -encode fgt.keytab tmp.b64 && findstr /v /c:- tmp.b64 > fgt.txt`
 - On Linux: `base64 fgt.keytab > fgt.txt`
 - On MacOS: `base64 -i fgt.keytab -o fgt.txt`
5. Use the code in `fgt.txt` as the keytab parameter when configuring the FortiGate.

Transparent web proxy forwarding

In FortiOS, there is an option to enable proxy forwarding for transparent web proxy policies and regular firewall policies for HTTP and HTTPS.

In previous versions of FortiOS, you could forward proxy traffic to another proxy server (proxy chaining) with explicit proxy. Now, you can forward web traffic to the upstream proxy without having to reconfigure your browsers or publish a proxy auto-reconfiguration (PAC) file.

Once configured, the FortiGate forwards traffic generated by a client to the upstream proxy. The upstream proxy then forwards it to the server.

To enable proxy forwarding using the CLI:

1. Configure the web proxy forwarding server:

```
config web-proxy forward-server
  edit "PC_03"
    set ip 172.16.200.46
    set healthcheck enable
    set monitor "http://www.google.ca"
```

```
        next
    end
```

2. Append the web proxy forwarding server to a firewall policy:

```
config firewall policy
    edit 1
        set name "LAN to WAN"
        set uuid b89f6184-2a6b-51e9-5e2d-9b877903a308
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set logtraffic all
        set webproxy-forward-server "PC_03"
        set fsso disable
        set av-profile "av"
        set ssl-ssh-profile "deep-custom"
        set nat enable
    next
end
```

Multiple dynamic header count

Multiple dynamic headers are supported for web proxy profiles, as well as Base64 encoding and the append/new options.

Administrators only have to select the dynamic header in the profile. The FortiGate will automatically display the corresponding static value. For example, if the administrator selects the `$client-ip` header, the FortiGate will display the actual client IP address.

The supported headers are:

<code>\$client-ip</code>	Client IP address
<code>\$user</code>	Authentication user name
<code>\$domain</code>	User domain name
<code>\$local_grp</code>	Firewall group name
<code>\$remote_grp</code>	Group name from authentication server
<code>\$proxy_name</code>	Proxy realm name

To configure dynamic headers using the CLI:

Since authentication is required, FSSO NTLM authentication is configured in this example.

1. Configure LDAP:

```
config user ldap
    edit "ldap-kerberos"
```

```
        set server "172.18.62.220"
        set cnid "cn"a
        set dn "dc=fortinetqa,dc=local"
        set type regular
        set username "CN=root,CN=Users,DC=fortinetqa,DC=local"
        set password *****
    next
end
```

2. Configure FSSO:

```
config user fsso
    edit "1"
        set server "172.18.62.220"
        set password *****
    next
end
```

3. Configure a user group:

```
config user group
    edit "NTLM-FSSO"
        set group-type fsso-service
        set member "FORTINETQA/FSSO"
    next
end
```

4. Configure an authentication scheme:

```
config authentication scheme
    edit "au-sch-ntlm"
        set method ntlm
    next
end
```

5. Configure an authentication rule:

```
config authentication rule
    edit "au-rule-fsso"
        set srcaddr "all"
        set active-auth-method "au-sch-ntlm"
    next
end
```

6. Create a web proxy profile that adds a new dynamic and custom Via header:

```
config web-proxy profile
    edit "test"
        set log-header-change enable
        config headers
            edit 1
                set name "client-ip"
                set content "$client-ip"
            next
            edit 2
                set name "Proxy-Name"
                set content "$proxy_name"
            next
            edit 3
                set name "user"
```

```

        set content "$user"
    next
    edit 4
        set name "domain"
        set content "$domain"
    next
    edit 5
        set name "local_grp"
        set content "$local_grp"
    next
    edit 6
        set name "remote_grp"
        set content "$remote_grp"
    next
    edit 7
        set name "Via"
        set content "Fortigate-Proxy"
    next
end
next
end

```

7. In the proxy policy, append the web proxy profile created in the previous step:

```

config firewall proxy-policy
    edit 1
        set uuid bb7488ee-2a6b-51e9-45c6-1715bdc271d8
        set proxy explicit-web
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set service "web"
        set action accept
        set schedule "always"
        set logtraffic all
        set groups "NTLM-FSSO"
        set webproxy-profile "test"
        set utm-status enable
        set av-profile "av"
        set webfilter-profile "content"
        set ssl-ssh-profile "deep-custom"
    next
end

```

8. Once traffic is being generated from the client, look at the web filter logs to verify that it is working. The corresponding values for all the added header fields displays in the *Change headers* section at the bottom of the *Log Details* pane.

```

1: date=2019-02-07 time=13:57:24 logid="0344013632" type="utm" subtype="webfilter"
eventtype="http_header_change" level="notice" vd="vdom1" eventtime=1549576642 policyid=1
transid=50331689 sessionid=1712788383 user="TEST21@FORTINETQA" group="NTLM-FSSO"
profile="test" srcip=10.1.100.116 srcport=53278 dstip=172.16.200.46 dstport=80
srcintf="port2" srcintfrole="undefined" dstintf="port1" dstintfrole="undefined" proto=6
service="HTTP" url="http://172.16.200.46/" agent="curl/7.22.0" chgheaders="Added=client-
ip: 10.1.100.116|Proxy-Name: 1.1 100D.qa|user: TEST21|domain: FORTINETQA|local_grp:
NTLM-FSSO|remote_grp: FORTINETQA/FSSO|Via: Fortigate-Proxy"

```


Date/Time	User	Source	Action	URL	Category/Description	Initiator	Sent / Received
2019/02/07 13:57:24	TEST21@FORTINETQA	TEST21@FORTINETQA(10.1.100.116)	http://...				
2019/02/07 13:57:24	TEST21@FORTINETQA	TEST21@FORTINETQA(10.1.100.116)	passthrough	172.1...			
2019/02/07 13:55:11	TEST21@FORTINETQA	TEST21@FORTINETQA(10.1.100.116)	http://...				
2019/02/07 13:55:11	TEST21@FORTINETQA	TEST21@FORTINETQA(10.1.100.116)	passthrough	172.1...			
2019/02/07 13:55:09	TEST21@FORTINETQA	TEST21@FORTINETQA(10.1.100.116)	http://...				
2019/02/07 13:55:09	TEST21@FORTINETQA	TEST21@FORTINETQA(10.1.100.116)	passthrough	172.1...			
2019/02/07 13:54:09	TEST21@FORTINETQA	TEST21@FORTINETQA(10.1.100.116)	blocked	172.1...			
2019/02/07 13:54:07	TEST21@FORTINETQA	TEST21@FORTINETQA(10.1.100.116)	http://...				
2019/02/07 13:54:07	TEST21@FORTINETQA	TEST21@FORTINETQA(10.1.100.116)	passthrough	172.1...			

Log Details	
IP	10.1.100.116
Source Port	53278
Source Interface	
User	
Group	NTLM-FSSO
Destination	
IP	172.16.200.46
Port	80
Destination Interface	
URL	
Application	
Protocol	6
Service	HTTP
Action	
Policy	
Security Level	
Other	
Sub Type	webfilter
Event Type	http_header_change
Log event	
original timestamp	1549576642
Transaction ID	50331689
Profile Name	test
Source Interface	undefined
Role	
Destination Interface	undefined
Role	
Change headers	Added-client-ip: 10.1.100.116(Proxy-Name: 1.1.100.0.qauser: TEST21@domain: FORTINETQA local_grp: NTLM-FSSO remote_grp: FORTINETQA FSSO Via: Fortigate-Proxy

Restricted SaaS access (Office 365, G Suite, Dropbox)

With the web proxy profile, you can specify access permissions for Microsoft Office 365, Google G Suite, and Dropbox. You can insert vendor-defined headers that restrict access to the specific accounts. You can also insert custom headers for any destination.

You can configure the web proxy profile with the required headers for the specific destinations, and then directly apply it to a policy to control the header's insertion.

To implement Office 365 tenant restriction, G Suite account access control, and Dropbox network access control:

1. Configure a web proxy profile according to the vendors' specifications:
 - a. Define the traffic destination (service provider).
 - b. Define the header name, defined by the service provider.
 - c. Define the value that will be inserted into the traffic, defined by your settings.
2. Apply the web proxy profile to a policy.

The following example creates a web proxy profile for Office 365, G Suite, and Dropbox access control.



Due to vendors' changing requirements, this example may no longer comply with the vendors' official guidelines.

To create a web proxy profile for access control using the CLI:

1. Configure the web proxy profile:

```
config web-proxy profile
edit "SaaS-Tenant-Restriction"
set header-client-ip pass
```

```

set header-via-request pass
set header-via-response pass
set header-x-forwarded-for pass
set header-front-end-https pass
set header-x-authenticated-user pass
set header-x-authenticated-groups pass
set strip-encoding disable
set log-header-change disable
config headers
    edit 1
        set name "Restrict-Access-To-Tenants" <----header name defined by
Office365 spec. input EXACTLY as it is
        set dstaddr "Microsoft Office 365" <----built-in destination address for
Office365
        set action add-to-request
        set base64-encoding disable
        set add-option new
        set protocol https http
        set content "contoso.onmicrosoft.com,fabrikam.onmicrosoft.com" <----
your tenants restriction configuration
    next
    edit 2
        set name "Restrict-Access-Context" <----header name defined by
Office365 spec. input EXACTLY as it is
        set dstaddr "Microsoft Office 365" <----built-in destination address
for Office365
        set action add-to-request
        set base64-encoding disable
        set add-option new
        set protocol https http
        set content "456ff232-3512-5h23-b3b3-3236w0826f3d" <----your directory
ID can find in Azure portal
    next
    edit 3
        set name "X-GooGApps-Allowed-Domains" <----header name defined by
Google G suite.
        set dstaddr "G Suite" <---- built-in G Suite destination address
        set action add-to-request
        set base64-encoding disable
        set add-option new
        set protocol https http
        set content "abcd.com" <----your domain restriction when you create G
Suite account
    next
    edit 4
        set name "X-Dropbox-allowed-Team-Ids" <----header defined by Dropbox
        set dstaddr "wildcard.dropbox.com" <----built-in destination address
for Dropbox
        set action add-to-request
        set base64-encoding disable
        set add-option new
        set protocol https http
        set content "dbmid:FDFS VF-DFSDF" <----your team-Id in Dropbox
    next
end

```

```
    next
end
```

2. Apply the web proxy profile to a firewall policy:

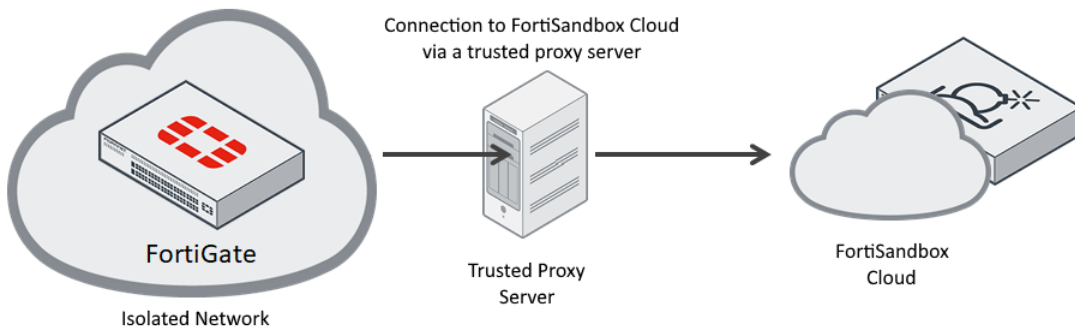
```
config firewall policy
  edit 1
    set name "WF"
    set srcintf "port10" "wifi"
    set dstintf "port9"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set webproxy-profile "SaaS-Tenant-Restriction"
    set utm-status enable
    set utm-inspection-mode proxy
    set logtraffic all
    set webfilter-profile "blocktest2"
    set application-list "g-default"
    set profile-protocol-options "protocol"
    set ssl-ssh-profile "protocols"
    set nat enable
  next
end
```

References

- Office 365: [Use tenant restrictions to manage access to SaaS cloud applications](#)
- G Suite: [Block access to consumer accounts](#)
- Dropbox: [Network control](#)

Explicit proxy and FortiSandbox Cloud

Explicit proxy connections can leverage FortiSandbox Cloud for advanced threat scanning and updates. This allows FortiGates behind isolated networks to connect to FortiCloud services.



To configure FortiGuard services to communicate with an explicit proxy server:

```
config system fortiguard
    set proxy-server-ip 172.16.200.44
    set proxy-server-port 3128
    set proxy-username "test1"
    set proxy-password ENC
Y0+KTg9UsILkv8+nDe+Pe3VlnlaHUMzLkfAXLATknW/xm/Xv7EdZHTnua1djM+wazA1vxCh8LV7Ci4sEhj/PABSTShSt
xskEn3E1+CjxviwVSljgF6AD+zJZF/+4jksqp+PogZT3LVO68+kqsPdU4rikuy1BbnsbZcPxC/MJyuIx7343bdKYqp+I
UprQUR2wf8tiMg==
end
```

To verify the explicit proxy connection to FortiSandbox Cloud:

```
# diagnose debug application forticldd -l
Debug messages will be on for 30 minutes.
# diagnose debug enable
[2942] fds_handle_request: Received cmd 23 from pid-2526, len 0
[40] fds_queue_task: req-23 is added to Cloud-sandbox-controller
[178] fds_svr_default_task_xmit: try to get IPs for Cloud-sandbox-controller
[239] fds_resolv_addr: resolve aptctrl1.fortinet.com
[169] fds_get_addr: name=aptctrl1.fortinet.com, id=32, cb=0x2bc089
[101] dns_parse_resp: DNS aptctrl1.fortinet.com -> 172.16.102.21
[227] fds_resolv_cb: IP-1: 172.16.102.21
[665] fds_ctx_set_addr: server: 172.16.102.21:443
[129] fds_svr_default_pickup_server: Cloud-sandbox-controller: 172.16.102.21:443
[587] fds_https_start_server: server: 172.16.102.21:443
[579] ssl_new: SSL object is created
[117] https_create: proxy server 172.16.200.44 port:3128
[519] fds_https_connect: https_connect(172.16.102.21) is established.
[261] fds_svr_default_on_established: Cloud-sandbox-controller has connected to
ip=172.16.102.21
[268] fds_svr_default_on_established: server-Cloud-sandbox-controller handles cmd-23
[102] fds_pack_objects: number of objects: 1
[75] fds_print_msg: FCPC: len=109
[81] fds_print_msg: Protocol=2.0
[81] fds_print_msg: Command=RegionList
[81] fds_print_msg: Firmware=FG101E-FW-6.02-0917
[81] fds_print_msg: SerialNumber=FG101E4Q17002429
[81] fds_print_msg: TimeZone=-7
[75] fds_print_msg: http req: len=248
[81] fds_print_msg: POST https://172.16.102.21:443/FCPSERVICE HTTP/1.1
[81] fds_print_msg: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
[81] fds_print_msg: Host: 172.16.102.21:443
[81] fds_print_msg: Cache-Control: no-cache
[81] fds_print_msg: Connection: close
[81] fds_print_msg: Content-Type: application/octet-stream
[81] fds_print_msg: Content-Length: 301
[524] fds_https_connect: http request to 172.16.102.21: header=248, ext=301.
[257] fds_https_send: sent 248 bytes: pos=0, len=248
[265] fds_https_send: 172.16.102.21: sent 248 byte header, now send 301-byte body
[257] fds_https_send: sent 301 bytes: pos=0, len=301
[273] fds_https_send: sent the entire request to server: 172.16.102.21:443
[309] fds_https_recv: read 413 bytes: pos=413, buf_len=2048
[332] fds_https_recv: received the header from server: 172.16.102.21:443, [HTTP/1.1 200
Content-Type: application/octet-stream
```

```
Content-Length: 279
Date: Thu, 20 Jun 2019 16:41:11 GMT
Connection: close]
[396] fds_https_recv: Do memmove buf_len=279, pos=279
[406] fds_https_recv: server: 172.16.102.21:443, buf_len=279, pos=279
[453] fds_https_recv: received a packet from server-172.16.102.21:443: sz=279, objs=1
[194] __ssl_data_ctx_free: Done
[839] ssl_free: Done
[830] ssl_disconnect: Shutdown
[481] fds_https_recv: obj-0: type=FCPR, len=87
[294] fds_svr_default_on_response: server-Cloud-sandbox-controller handles cmd-23
[75] fds_print_msg: fcpr: len=83
[81] fds_print_msg: Protocol=2.0
[81] fds_print_msg: Response=202
[81] fds_print_msg: ResponseItem=Region:Europe,Global,Japan,US
[81] fds_print_msg: existing:Japan
[3220] aptctrl_region_res: Got rsp: Region:Europe,Global,Japan,US
[3222] aptctrl_region_res: Got rsp: Region existing:Japan
[439] fds_send_reply: Sending 28 bytes data.
[395] fds_free_tsk: cmd=23; req.noreply=1
# [136] fds_on_sys_fds_change: trace
[2942] fds_handle_request: Received cmd 22 from pid-170, len 0
[40] fds_queue_task: req-22 is added to Cloud-sandbox-controller
[587] fds_https_start_server: server: 172.16.102.21:443
[579] ssl_new: SSL object is created
[117] https_create: proxy server 172.16.200.44 port:3128
[519] fds_https_connect: https_connect(172.16.102.21) is established.
[261] fds_svr_default_on_established: Cloud-sandbox-controller has connected to
ip=172.16.102.21
[268] fds_svr_default_on_established: server-Cloud-sandbox-controller handles cmd-22
[102] fds_pack_objects: number of objects: 1
[75] fds_print_msg: FCPC: len=146
[81] fds_print_msg: Protocol=2.0
[81] fds_print_msg: Command=UpdateAPT
[81] fds_print_msg: Firmware=FG101E-FW-6.02-0917
[81] fds_print_msg: SerialNumber=FG101E4Q17002429
[81] fds_print_msg: TimeZone=-7
[81] fds_print_msg: TimeZoneInMin=-420
[81] fds_print_msg: DataItem=Region:US
[75] fds_print_msg: http req: len=248
[81] fds_print_msg: POST https://172.16.102.21:443/FCPSERVICE HTTP/1.1
[81] fds_print_msg: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
[81] fds_print_msg: Host: 172.16.102.21:443
[81] fds_print_msg: Cache-Control: no-cache
[81] fds_print_msg: Connection: close
[81] fds_print_msg: Content-Type: application/octet-stream
[81] fds_print_msg: Content-Length: 338
[524] fds_https_connect: http request to 172.16.102.21: header=248, ext=338.
[257] fds_https_send: sent 248 bytes: pos=0, len=248
[265] fds_https_send: 172.16.102.21: sent 248 byte header, now send 338-byte body
[257] fds_https_send: sent 338 bytes: pos=0, len=338
[273] fds_https_send: sent the entire request to server: 172.16.102.21:443
[309] fds_https_recv: read 456 bytes: pos=456, buf_len=2048
[332] fds_https_recv: received the header from server: 172.16.102.21:443, [HTTP/1.1 200
Content-Type: application/octet-stream
Content-Length: 322
```

```
Date: Thu, 20 Jun 2019 16:41:16 GMT
Connection: close]
[396] fds_https_recv: Do memmove buf_len=322, pos=322
[406] fds_https_recv: server: 172.16.102.21:443, buf_len=322, pos=322
[453] fds_https_recv: received a packet from server-172.16.102.21:443: sz=322, objs=1
[194] __ssl_data_ctx_free: Done
[839] ssl_free: Done
[830] ssl_disconnect: Shutdown
[481] fds_https_recv: obj-0: type=FCPR, len=130
[294] fds_svr_default_on_response: server-Cloud-sandbox-controller handles cmd-22
[75] fds_print_msg: fcpr: len=126
[81] fds_print_msg: Protocol=2.0
[81] fds_print_msg: Response=202
[81] fds_print_msg: ResponseItem=Server1:172.16.102.51:514
[81] fds_print_msg: Server2:172.16.102.52:514
[81] fds_print_msg: Contract:20210215
[81] fds_print_msg: NextRequest:86400
[615] parse Apt_contract_time_str: The APTContract is valid to Mon Feb 15 23:59:59 2021
[616] parse Apt_contract_time_str: FGT current local time is Thu Jun 20 09:41:16 2019
[3289] aptctrl_update_res: Got rsp: APT=172.16.102.51:514 APTAlter=172.16.102.52:514 next-
upd=86400
[395] fds_free_tsk: cmd=22; req.noreply=1
```

DHCP server

A DHCP server provides an address from a defined address range to a client on the network, when requested.

You can configure one or more DHCP servers on any FortiGate interface. A DHCP server dynamically assigns IP addresses to hosts on the network connected to the interface. The host computers must be configured to obtain their IP addresses using DHCP.

You can configure a FortiGate interface as a DHCP relay. The interface forwards DHCP requests from DHCP clients to an external DHCP server and returns the responses to the DHCP clients. The DHCP server must have appropriate routing so that its response packets to the DHCP clients arrive at the unit.

Configure DHCP on the FortiGate

To add a DHCP server on the GUI:

1. Go to *Network > Interfaces*.
2. Edit an interface.
3. Enable the *DHCP Server* option and configure the settings.

To add a DHCP server on the CLI:

```
config system dhcp server
  edit 1
    set dns-service default
    set default-gateway 192.168.1.2
    set netmask 255.255.255.0
    set interface "port1"
```

```
config ip-range
  edit 1
    set start-ip 192.168.1.1
    set end-ip 192.168.1.1
  next
  edit 2
    set start-ip 192.168.1.3
    set end-ip 192.168.1.254
  next
end
set timezone-option default
set tftp-server "172.16.1.2"
next
end
```

DHCP options

When adding a DHCP server, you can include DHCP codes and options. The DHCP options are BOOTP vendor information fields that provide additional vendor-independent configuration parameters to manage the DHCP server. For example, you might need to configure a FortiGate DHCP server that gives out a separate option as well as an IP address, such as an environment that needs to support PXE boot with Windows images.

The option numbers and codes are specific to the application. The documentation for the application indicates the values to use. Option codes are represented in a option value/HEX value pairs. The option is a value between 1 and 255.

You can add up to three DHCP code/option pairs per DHCP server.

To configure option 252 with value `http://192.168.1.1/wpad.dat` using the CLI:

```
config system dhcp server
  edit <server_entry_number>
    set option1 252 687474703a2f2f3139322e3136382e312e312f777061642e646174
  next
end
```

For detailed information about DHCP options, see [RFC 2132](#), DHCP Options and BOOTP Vendor Extensions.

Option 82

The DHCP relay agent information option (option 82 in [RFC 3046](#)) helps protect the FortiGate against attacks such as spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address starvation.

This option is disabled by default. However, when `dhcp-relay-service` is enabled, `dhcp-relay-agent-option` becomes enabled.

To configure the DHCP relay agent option using the CLI:

```
config system interface
  edit <interface>
    set vdom root
    set dhcp-relay-service enable
    set dhcp-relay-ip <ip>
    set dhcp-relay-agent-option enable
    set vlanid <id>
```

```

    next
end

```

See [IP address assignment with relay agent information option](#) on page 402 for an example.

Option 42

This option specifies a list of the NTP servers available to the client by IP address.

```

config system dhcp server
    edit 2
        set ntp-service {local | default | specify}
        set ntp-server1 <class_ip>
        set ntp-server2 <class_ip>
        set ntp-server3 <class_ip>
    next
end

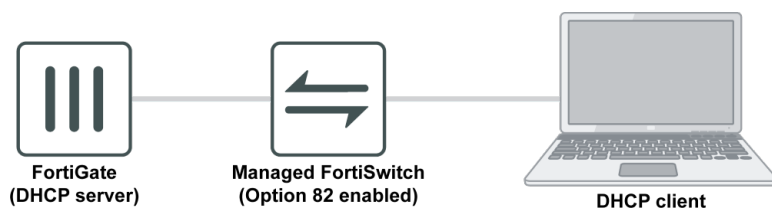
```

The NTP service options include:

- **local:** The IP address of the interface that the DHCP server is added to becomes the client's NTP server IP address.
- **default:** Clients are assigned the FortiGate's configured NTP servers.
- **specify:** Specify up to three NTP servers in the DHCP server configuration.

IP address assignment with relay agent information option

Option 82 (DHCP relay information option) helps protect the FortiGate against attacks such as spoofing (or forging) of IP and MAC addresses, and DHCP IP address starvation.



The following CLI variables are included in the `config system dhcp server> config reserved-address` command:

<code>circuit-id-type {hex string}</code>	DHCP option type; hex or string (default).
<code>circuit-id <value></code>	Option 82 circuit ID of the client that will get the reserved IP address. Format: <i>vlan-mod-port</i> <ul style="list-style-type: none"> • vlan: VLAN ID (2 bytes) • mod: 1 = snoop, 0 = relay (1 byte) • port: port number (1 byte)
<code>remote-id-type {hex string}</code>	DHCP option type; hex or string (default).
<code>remote-id <value></code>	Option 82 remote ID of the client that will get the reserved IP address. Format: the MAC address of the client.


```
type {mac | option82}
```

The DHCP reserved address type; mac (default) or option82.

To create an IP address assignment rule using option 82 in the GUI:

1. Go to *Network > Interfaces*.
2. Edit an existing port, or create a new one.



The port *Role* must be *LAN* or *Undefined*.

3. Enable *DHCP Server*.
4. Configure the address ranges and other settings as needed.
5. Click + to expand the *Advanced* options.
6. In the *IP Address Assignment Rules* table, click *Create New*.

FortiGate VM64 FGM00TM19000872

Dashboard > Security Fabric > FortiView > Network > Interfaces > Edit Interface

☒ DHCP Server

Address Range

Starting IP	End IP
100.100.100.1	100.100.100.99
100.100.100.101	100.100.100.254

Netmask: 255.255.255.0

Default Gateway: Same as Interface IP Specify

DNS Server: Same as System DNS Same as Interface IP Specify

Advanced...

Mode: Server Relay

NTP Server: Local Same as System NTP Specify

Time Zone: Same as System Specify

Next Bootstrap Server: 0.0.0.0

Type: Regular IPsec

Additional DHCP Options

Seq #	Option Code	Value	Hexadecimal Value
51 (Lease Time)	604800		

IP Address Assignment Rules

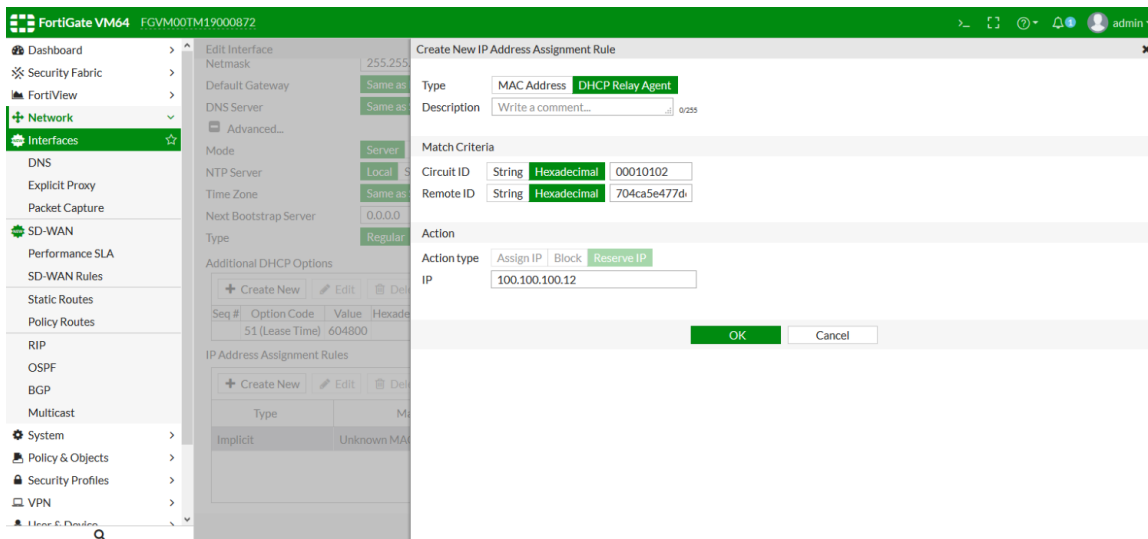
Type	Match Criteria	Action	IP
Implicit	Unknown MAC Addresses	Assign IP	

Return OK Cancel

The *Create New IP Address Assignment Rule* pane opens.

7. Configure the new rule:
 - a. For the *Type*, select *DHCP Relay Agent*.
 - b. Enter the *Circuit ID* and *Remote ID*.
 - c. Enter the *IP* address that will be reserved.

8. Click OK.



To create an IP address assignment rule using option 82 with the CLI:

```
config system dhcp server
  edit 1
    set netmask 255.255.255.0
    set interface "port4"
    config ip-range
      edit 1
        set start-ip 100.100.100.1
        set end-ip 100.100.100.99
      next
      edit 2
        set start-ip 100.100.100.101
        set end-ip 100.100.100.254
      next
    end
    config reserved-address
      edit 1
        set type option82
        set ip 100.100.100.12
        set circuit-id-type hex
        set circuit-id "00010102"
        set remote-id-type hex
        set remote-id "704ca5e477d6"
      next
    end
  next
end
```

Static routing

Static routing is one of the foundations of firewall configuration. It is a form of routing in which a device uses manually-configured routes. In the most basic setup, a firewall will have a default route to its gateway to provide network access. In a more complex setup with dynamic routing, ADVPN, or SD-WAN involved, you would still likely find static routes being deployed.

This section explores concepts in using static routing and provides examples in common use cases:

- [Routing concepts on page 405](#)
- [Policy routes on page 415](#)
- [Equal cost multi-path on page 417](#)
- [Dual internet connections on page 421](#)

The following topics include additional information about static routes:

- [Deploying the Security Fabric on page 103](#)
- [Security Fabric over IPsec VPN on page 111](#)
- [Viewing and controlling network risks via topology view on page 101](#)
- [Adding a static route on page 454](#)
- [Configure VDOM-A on page 658](#)
- [Configure VDOM-A on page 667](#)
- [IPsec VPN in an HA environment on page 1256](#)
- [IPsec VPN to Azure with virtual network gateway on page 1177](#)
- [FortiGate as dialup client on page 1199](#)
- [ADVPN with BGP as the routing protocol on page 1314](#)
- [ADVPN with OSPF as the routing protocol on page 1323](#)
- [ADVPN with RIP as the routing protocol on page 1332](#)
- [Basic site-to-site VPN with pre-shared key on page 1140](#)
- [Site-to-site VPN with digital certificate on page 1145](#)
- [Tunneled Internet browsing on page 1231](#)
- [FortiGate multiple connector support on page 1667](#)
- [IPsec aggregate for redundancy and traffic load-balancing on page 1262](#)
- [Using BGP tags with SD-WAN rules on page 518](#)

Routing concepts

This section contains the following topics:

- [Default route on page 406](#)
- [Adding or editing a static route on page 406](#)
- [Configuring FQDNs as a destination address in static routes on page 407](#)
- [Routing table on page 407](#)
- [Viewing the routing database on page 410](#)
- [Kernel routing table on page 411](#)
- [Route cache on page 412](#)
- [Route look-up on page 412](#)

- [Blackhole routes on page 413](#)
- [Reverse path look-up on page 414](#)
- [Asymmetric routing on page 414](#)
- [Routing changes on page 415](#)

Default route

The default route has a destination of `0.0.0.0/0.0.0.0`, representing the least specific route in the routing table. It is a catch all route in the routing table when traffic cannot match a more specific route. Typically this is configured with a static route with an administrative distance of `10`. In most instances, you will configure the next hop interface and the gateway address pointing to your next hop. If your FortiGate is sitting at the edge of the network, your next hop will be your ISP gateway. This provides internet access for your network.

Sometimes the default route is configured through DHCP. On some desktop models, the WAN interface is preconfigured in DHCP mode. Once the WAN interface is plugged into the network modem, it will receive an IP address, default gateway, and DNS server. FortiGate will add this default route to the routing table with a distance of `5`, by default. This will take precedence over any default static route with a distance of `10`. Therefore, take caution when you are configuring an interface in DHCP mode, where *Retrieve default gateway from server* is enabled. You may disable it and/or change the distance from the *Network > Interfaces* page when you edit an interface.

Adding or editing a static route

To add a static route using the GUI:

1. Go to *Network > Static Routes* and click *Create New*.
2. Enter the following information:

Dynamic Gateway	When enabled, a selected DHCP/PPPoE interface will automatically retrieve its dynamic gateway.
Destination	<ul style="list-style-type: none"> • Subnet Enter the destination IP address and netmask. A value of <code>0.0.0.0/0.0.0.0</code> creates a default route. • Named Address Select an address or address group object. Only addresses with static route configuration enabled will appear on the list. This means a geography type address cannot be used. • Internet Service Select an Internet Service. These are known IP addresses of popular services across the Internet.
Interface	Select the name of the interface that the static route will connect through.
Gateway Address	Enter the gateway IP address. When selecting an IPsec VPN interface or SD-WAN creating a blackhole route, the gateway cannot be specified.
Administrative Distance	Enter the distance value, which will affect which routes are selected first by different protocols for route management or load balancing. The default is <code>10</code> .

Advanced Options

Optionally, expand *Advanced Options* and enter a *Priority*. When two routes have an equal distance, the route with a lower priority number will take precedence. The default is 0.

3. Click **OK**.

Configuring FQDNs as a destination address in static routes

You can configure FQDN firewall addresses as destination addresses in a static route, using either the GUI or the CLI.

In the GUI, to add an FQDN firewall address to a static route in the firewall address configuration, enable the *Static Route Configuration* option. Then, when you configure the static route, set *Destination* to *Named Address*.

To configure an FQDN as a destination address in a static route using the CLI:

```
config firewall address
  edit 'Fortinet-Documentation-Website'
    set type fqdn
    set fqdn docs.fortinet.com
    set allow-routing enable
  end
config router static
  edit 0
    set dstaddr Fortinet-Documentation-Website
    ...
end
```

Routing table

A routing table consists of only the best routes learned from the different routing protocols. The most specific route always takes precedence. If there is a tie, then the route with a lower administrative distance will be injected into the routing table. If administrative distances are also equal, then all the routes are injected into the routing table, and *Cost* and *Priority* become the deciding factors on which a route is preferred. If these are also equal, then FortiGate will use [Equal cost multi-path on page 417](#) to distribute traffic between these routes.

Viewing the routing table in the GUI

You can view routing tables in the FortiGate GUI under *Monitor > Routing Monitor* by default. You can also monitor policy routes by toggling from *Static & Dynamic* to *Policy* from the toolbar on the top left of the page. The active policy routes include policy routes that you created, SD-WAN rules, and Internet Service static routes. It also supports downstream devices in the Security Fabric.

The following screenshot shows an example of the static and dynamic routes under *Monitor > Routing Monitor*.

Refresh

Route Lookup

View

Create Address

Search

Static & Dynamic

Policy

Branch_Office_02

Type	Network	Gateway IP	Interfaces	Distance	Metric	Up Since
Static	0.0.0.0/0	10.10.11.1	To-HQ-B	1	0	
Static	0.0.0.0/0	10.0.10.1	To-HQ-A	1	0	
Static	0.0.0.0/0	10.0.12.1	To-HQ-MPLS	1	0	
Static	0.0.0.0/0	10.100.68.1	Internet_A (port1)	1	0	
Static	0.0.0.0/0	10.100.68.9	Internet_B (port2)	1	0	
Connected	10.0.10.0/24	0.0.0.0	To-HQ-A	0	0	
Connected	10.0.10.3/32	0.0.0.0	To-HQ-A	0	0	
Connected	10.0.11.0/24	0.0.0.0	To-HQ-B	0	0	
Connected	10.0.11.3/32	0.0.0.0	To-HQ-B	0	0	
Connected	10.0.12.0/24	0.0.0.0	To-HQ-MPLS	0	0	
Connected	10.0.12.3/32	0.0.0.0	To-HQ-MPLS	0	0	
BGP	10.1.0.0/24	10.0.10.2	To-HQ-A	200	0	11 hours ago
BGP	10.1.0.0/24	10.0.11.2	To-HQ-B	200	0	11 hours ago
Connected	10.2.0.0/24	0.0.0.0	B02_LAN (port3)	0	0	
Connected	10.2.0.2/32	0.0.0.0	B02_LAN (port3)	0	0	

0% 57 | Updated: 11:58:46

Refresh

To view more columns, right-click on the column header to select the columns to be displayed:

Field	Description
Type	<p>The type values assigned to FortiGate routes (Static, Connected, RIP, OSPF, or BGP):</p> <ul style="list-style-type: none"> Connected: All routes associated with direct connections to FortiGate interfaces Static: The static routes that have been added to the routing table manually RIP: All routes learned through RIP RIPNG: All routes learned through RIP version 6 (which enables the sharing of routes through IPv6 networks) BGP: All routes learned through BGP OSPF: All routes learned through OSPF OSPF6: All routes learned through OSPF version 6 (which enables the sharing of routes through IPv6 networks) IS-IS: All routes learned through IS-IS HA: RIP, OSPF, and BGP routes synchronized between the primary unit and the subordinate units of a high availability (HA) cluster. HA routes are maintained on subordinate units and are visible only if you're viewing the router monitor from a virtual domain that is configured as a subordinate virtual domain in a virtual cluster.
Network	The IP addresses and network masks of destination networks that the FortiGate can reach.
Gateway IP	The IP addresses of gateways to the destination networks.
Interfaces	The interface through which packets are forwarded to the gateway of the destination network.
Distance	The administrative distance associated with the route. A lower value means the route is preferable compared to other routes to the same destination.

Field	Description
Metric	<p>The metric associated with the route type. The metric of a route influences how the FortiGate dynamically adds it to the routing table. The following are types of metrics and the protocols they are applied to:</p> <ul style="list-style-type: none"> • <i>Hop count</i>: Routes learned through RIP • <i>Relative cost</i>: Routes learned through OSPF • <i>Multi-Exit Discriminator (MED)</i>: Routes learned through BGP. By default, the MED value associated with a BGP route is zero. However, the MED value can be modified dynamically. If the value was changed from the default, the Metric column displays a non-zero value.
Up Since	The total accumulated amount of time that a route learned through RIP, OSPF, or BGP has been reachable.

Viewing the routing table in the CLI

Viewing the routing table using the CLI displays the same routes as you would see from the GUI.

If VDOMs are enabled on the FortiGate, all routing-related CLI commands must be run within a VDOM and not in the global context.

To view the routing table using the CLI:

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S* 0.0.0.0/0 [1/0] via 172.31.0.1, MPLS [1/0]
   via 192.168.2.1, port1 [1/0] via 192.168.122.1, port2
S 1.2.3.4/32 [10/0] via 172.16.100.81, VLAN100
C 10.10.2.0/24 is directly connected, hub
C 10.10.2.1/32 is directly connected, hub
O 10.10.10.0/24 [110/101] via 192.168.2.1, port1, 01:54:18
C 10.253.240.0/20 is directly connected, wqt.root
S 110.2.2.122/32 [22/0] via 2.2.2.2, port2, [3/3]
C 172.16.50.0/24 is directly connected, WAN1-VLAN50
C 172.16.60.0/24 is directly connected, WAN2-VLAN60
C 172.16.100.0/24 is directly connected, VLAN100
C 172.31.0.0/30 is directly connected, MPLS
C 172.31.0.2/32 is directly connected, MPLS
B 192.168.0.0/24 [20/0] via 172.31.0.1, MPLS, 00:31:43
C 192.168.2.0/24 is directly connected, port1
C 192.168.20.0/24 is directly connected, port3
C 192.168.99.0/24 is directly connected, Port1-VLAN99
C 192.168.122.0/24 is directly connected, port2
Routing table for VRF=10
C 172.16.101.0/24 is directly connected, VLAN101
```

Examining an entry:

B 192.168.0.0/24 [20/0] via 172.31.0.1, MPLS, 00:31:43

Value	Description
B	BGP. The routing protocol used.
192.168.0.0/24	The destination of this route, including netmask.
[20/0]	20 indicates an administrative distance of 20 out of a range of 0 to 255. 0 is an additional metric associated with this route, such as in OSPF.
172.31.0.1	The gateway or next hop.
MPLS	The interface that the route uses.
00:31:43	The age of the route in HH:MM:SS.

Viewing the routing database

The routing database consists of all learned routes from all routing protocols before they are injected into the routing table. This likely lists more routes than the routing table as it consists of routes to the same destinations with different distances. Only the best routes are injected into the routing table. However, it is useful to see all learned routes for troubleshooting purposes.

To view the routing database using the CLI:

```
# get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S *> 0.0.0.0/0 [1/0] via 172.31.0.1, MPLS
    *> [1/0] via 192.168.2.1, port1
    *> [1/0] via 192.168.122.1, port2
S *> 1.2.3.4/32 [10/0] via 172.16.100.81, VLAN100
C *> 10.10.2.0/24 is directly connected, hub
C *> 10.10.2.1/32 is directly connected, hub
O *> 10.10.10.0/24 [110/101] via 192.168.2.1, port1, 02:10:17
C *> 10.253.240.0/20 is directly connected, wqt.root
S *> 110.2.2.122/32 [22/0] via 2.2.2.2, port2, [3/3]
C *> 172.16.50.0/24 is directly connected, WAN1-VLAN50
C *> 172.16.60.0/24 is directly connected, WAN2-VLAN60
C *> 172.16.100.0/24 is directly connected, VLAN100
O 172.31.0.0/30 [110/201] via 192.168.2.1, port1, 00:47:36
C *> 172.31.0.0/30 is directly connected, MPLS
```

Selected routes are marked by the > symbol. In the above example, the OSPF route to destination 172.31.0.0/30 is not selected.

Kernel routing table

The kernel routing table makes up the actual Forwarding Information Base (FIB) that used to make forwarding decisions for each packet. The routes here are often referred to as kernel routes. Parts of this table are derived from the routing table that is generated by the routing daemon.

To view the kernel routing table using the CLI:

```
# get router info kernel
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0
    gwy=172.31.0.1 flag=04 hops=0 oif=31(MPLS) gwy=192.168.2.1 flag=04 hops=0 oif=3(port1)
    gwy=192.168.122.1 flag=04 hops=0 oif=4(port2)
tab=254 vf=0 scope=0 type=1 proto=17 prio=0 192.168.122.98/255.255.255.255/0->1.1.1.1/32
    pref=0.0.0.0 gwy=192.168.122.1 dev=4(port2)
tab=254 vf=0 scope=0 type=1 proto=17 prio=0 172.31.0.2/255.255.255.255/0->1.1.1.1/32
    pref=0.0.0.0 gwy=172.31.0.1 dev=31(MPLS)
tab=254 vf=0 scope=0 type=1 proto=17 prio=0 192.168.2.5/255.255.255.255/0->1.1.1.1/32
    pref=0.0.0.0 gwy=192.168.2.1 dev=3(port1)
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->1.2.3.4/32 pref=0.0.0.0
    gwy=172.16.100.81 dev=20(VLAN100)
tab=254 vf=0 scope=0 type=1 proto=17 prio=0 192.168.122.98/255.255.255.255/0->8.8.8.8/32
    pref=0.0.0.0 gwy=192.168.122.1 dev=4(port2)
```

The kernel routing table entries are:

Value	Description
tab	Table number: It will either be 254 (unicast) or 255 (multicast).
vf	Virtual domain of the firewall: It is the VDOM index number. If VDOMs are not enabled, this number is 0.
type	Type of routing connection. Valid values include: <ul style="list-style-type: none"> 0 - unspecified 1 - unicast 2 - local 3 - broadcast 4 - anycast 5 - multicast 6 - blackhole 7 - unreachable 8 - prohibited
proto	Type of installation that indicates where the route came from. Valid values include: <ul style="list-style-type: none"> 0 - unspecified 2 - kernel 11 - ZebOS routing module 14 - FortiOS 15 - HA 16 - authentication based 17 - HA1

Value	Description
prio	Priority of the route. Lower priorities are preferred.
->0.0.0.0/0 (->x.x.x.x/mask)	The IP address and subnet mask of the destination.
pref	Preferred next hop along this route.
gwy	Gateway: The address of the gateway this route will use.
dev	Outgoing interface index: This number is associated with the interface for this route. If VDOMs are enabled, the VDOM is also included here. If an interface alias is set for this interface, it is also displayed here.

Route cache

The route cache contains recently used routing entries in a table. It is consulted before the routing table to speed up the route look-up process.

To view the route cache using the CLI:

```
# diagnose ip rtcache list
family=02 tab=254 vrf=0 vf=0 type=01 tos=0 flag=00000200
  0.0.0.0@0->208.91.113.230@3(port1) gwy=192.168.2.1 prefsrc=192.168.2.5
  ci: ref=0 lastused=1 expire=0 err=00000000 used=5 br=0 pmtu=1500
family=02 tab=254 vrf=0 vf=0 type=01 tos=0 flag=00000200
  192.168.2.5@0->8.8.8.8@3(port1) gwy=192.168.2.1 prefsrc=0.0.0.0
  ci: ref=0 lastused=0 expire=0 err=00000000 used=2 br=0 pmtu=1500
family=02 tab=254 vrf=0 vf=0 type=02 tos=8 flag=80000200
  8.8.8.8@31(MPLS)->172.31.0.2@6(root) gwy=0.0.0.0 prefsrc=172.31.0.2
  ci: ref=1 lastused=0 expire=0 err=00000000 used=0 br=0 pmtu=16436
family=02 tab=254 vrf=0 vf=0 type=02 tos=0 flag=84000200
  192.168.20.6@5(port3)->192.168.20.5@6(root) gwy=0.0.0.0 prefsrc=192.168.20.5
  ci: ref=2 lastused=0 expire=0 err=00000000 used=1 br=0 pmtu=16436
...
```

The size of the route cache is calculated by the kernel. However, you can modify it.

To modify the size of the route cache:

```
# config system global
  set max-route-cache-size <number_of_cache_entries>
end
```

Route look-up

Route look-up typically occurs twice in the life of a session. Once when the first packet is sent by the originator and once more when the first reply packet is sent from the responder. When a route look-up occurs, the routing information is written to the session table and the route cache. If routing changes occur during the life of a session, additional routing look-ups may occur.

FortiGate performs a route look-up in the following order:

1. Policy-based routes: If a match occurs and the action is to forward, traffic is forwarded based on the policy route.
2. Route Cache: If there are no matches, FortiGate looks for the route in the route cache.
3. Forwarding Information Base, otherwise known as the kernel routing table.
4. If no match occurs, the packet is dropped.

Searching the routing table

When there are many routes in your routing table, you can perform a quick search by using the search bar to specify your criteria, or apply filters on the column header to display only certain routes. For example, if you want to only display static routes, you may use "static" as the search term, or filter by the *Type* field with value *Static*.

Route look-up on the other hand provides a utility for you to enter criteria such as *Destination*, *Destination Port*, *Source*, *Protocol* and/or *Source Interface*, in order to determine the route that a packet will take. Once you click *Search*, the corresponding route will be highlighted.

You can also use the CLI for a route look-up. The CLI provides a basic route look-up tool.

To look-up a route using the CLI:

```
# get router info routing-table details 4.4.4.4
Routing table for VRF=0
Routing entry for 0.0.0.0/0
    Known via "static", distance 1, metric 0, best
    * 172.31.0.1, via MPLS distance 0
    * 192.168.2.1, via port1 distance 0
    * 192.168.122.1, via port2 distance 0
```

Blackhole routes

Sometimes upon routing table changes, it is not desirable for traffic to be routed to a different gateway. For example, you may have traffic destined for a remote office routed through your IPsec VPN interface. When the VPN is down, traffic will try to re-route to another interface. However, this may not be viable and traffic will instead be routed to your default route through your WAN, which is not desirable. Traffic may also be routed to another VPN, which you do not want. For such scenarios, it is good to define a blackhole route so that traffic is dropped when your desired route is down. Upon reconnection, your desired route is once again added to the routing table and your traffic will resume routing to your desired interface. For this reason, blackhole routes are created when you configure an IPsec VPN using the IPsec wizard.

To create a blackhole route from the GUI:

1. Go to *Network > Static Routes*.
2. Click *Create New*. The *New Static Route* screen appears.
3. Specify a *Destination* type.
4. Select *Blackhole* from the *Interface* field.
5. Type the desired *Administrative Distance*.
6. Click *OK*.



Route priority for a *Blackhole* route can only be configured from the CLI.

Reverse path look-up

Whenever a packet arrives at one of the interfaces on a FortiGate, the FortiGate determines whether the packet was received on a legitimate interface by doing a reverse look-up using the source IP address in the packet header. This protects against IP spoofing attacks. If the FortiGate does not have a route to the source IP address through the interface on which the packet was received, the FortiGate drops the packet as per Reverse Path Forwarding (RPF) check. There are two modes of RPF – feasible path and strict. The default feasible RPF mode checks only for the existence of at least one active route back to the source using the incoming interface. The strict RPF check ensures the best route back to the source is used as the incoming interface.

To configure a strict Reverse Path Forwarding check using the CLI:

```
# config system settings
  set strict-src-check enable
end
```

You can remove RPF state checks without needing to enable asymmetric routing by disabling state checks for traffic received on specific interfaces. Disabling state checks makes a FortiGate less secure and should only be done with caution for troubleshooting purposes.

To remove Reverse Path Forwarding checks from the state evaluation process using the CLI:

```
# config system interface
  edit <interface_name>
    set src-check disable
  next
end
```

Asymmetric routing

The firewall tries to ensure symmetry in its traffic by using the same source-destination combination in the original and reverse path. Asymmetric routing occurs when traffic in the returning direction takes a different path than the original. There may be various scenarios in which this happens. For example, traffic in the original direction hits the firewall on `port1`, and is routed to `port2`. However, returning traffic is received on `port3` instead. In this scenario, asymmetric routing occurs and the returning traffic is blocked.

If for some specific reason it is required that a FortiGate unit should permit asymmetric routing, you can configure it by using CLI commands per VDOM.

To configure asymmetric routing per VDOM by using the CLI:

```
# config vdom
  edit <vdom_name>
    config system settings
      set asymroute enable
    end
  next
end
```

Routing changes

When routing changes occur, routing look-up may occur on an existing session depending on certain configurations.

Routing Changes without SNAT

When a routing change occurs, FortiGate flushes all routing information from the session table and performs new routing look-up for all new packets on arrival by default. You can modify the default behavior using the following commands:

```
# config system interface
  edit <interface>
    set preserve-session-route enable
  next
end
```

By enabling `preserve-session-route`, the FortiGate marks existing session routing information as persistent. Therefore, routing look-up only occurs on new sessions.

Routing Changes with SNAT

When SNAT is enabled, the default behavior is opposite to that of when SNAT is not enabled. After a routing change occurs, sessions with SNAT keep using the same outbound interface as long as the old route is still active. This may be the case if the priority of the static route was changed. You can modify this default behavior using the following commands:

```
# config system global
  set snat-route-change enable
end
```

By enabling `snat-route-change`, sessions with SNAT will require new route look-up when a routing change occurs. This will apply a new SNAT to the session.

Policy routes

Policy routing allows you to specify an interface to route traffic. This is useful when you need to route certain types of network traffic differently than you would if you were using the routing table. You can use the incoming traffic's protocol, source or destination address, source interface, or port number to determine where to send the traffic.

When a packet arrives, the FortiGate starts at the top of the policy route list and attempts to match the packet with a policy. For a match to be found, the policy must contain enough information to route the packet. At a minimum, this requires the outgoing interface to forward the traffic, and the gateway to route the traffic to. If one or both of these are not specified in the policy route, then the FortiGate searches the routing table to find the best active route that corresponds to the policy route. If no routes are found in the routing table, then the policy route does not match the packet. The FortiGate continues down the policy route list until it reaches the end. If no matches are found, then the FortiGate does a route lookup using the routing table.



Policy routes are sometimes referred to as Policy-based routes (PBR).

Configuring a policy route

In this example, a policy route is configured to send all FTP traffic received at port1 out through port4 and to a next hop router at 172.20.120.23. To route FTP traffic, the protocol is set to TCP (6) and the destination ports are set to 21 (the FTP port).

To configure a policy route in the GUI:

1. Go to *Network > Policy Routes*.
2. Click *Create New > Policy Route*.
3. Configure the following fields:

Incoming interface	port1
Source Address	0.0.0.0/0.0.0.0
Destination Address	0.0.0.0/0.0.0.0
Protocol	TCP
Destination ports	21 - 21
Type of service	0x00
Bit Mask	0x00
Outgoing interface	Enable and select port4
Gateway address	172.20.120.23

The screenshot shows the 'New Routing Policy' configuration window. Under 'If incoming traffic matches:', the Incoming Interface is 'port1', Source Address is '0.0.0.0/0.0.0.0', Destination Address is '0.0.0.0/0.0.0.0', Protocol is 'TCP', Source ports are '0 - 65535', and Destination ports are '21 - 21'. Under 'Then:', the Action is 'Forward Traffic', Outgoing interface is 'port4', Gateway address is '172.20.120.23', and the Status is 'Enabled'.

4. Click **OK**.

To configure a policy route in the CLI:

```
config router policy
  edit 1
    set input-device "port1"
    set src "0.0.0.0/0.0.0.0"
    set dst "0.0.0.0/0.0.0.0"
```

```

        set protocol 6
        set start-port 21
        set end-port 21
        set gateway 172.20.120.23
        set output-device "port4"
        set tos 0x00
        set tos-mask 0x00
    next
end

```

Moving a policy route

A routing policy is added to the bottom of the table when it is created. Routing policies can be moved to a different location in the table to change the order of preference. In this example, routing policy 3 will be moved before routing policy 2.

To move a policy route in the GUI:

1. Go to *Network > Policy Routes*.
2. In the table, select the policy route.

<div> <div>+ Create New</div> <div>Edit</div> <div>Delete</div> <div>Search</div> <div>Q</div> </div>					
Seq.#	Incoming Interface	Outgoing Interface	Source	Destination	Hit Count
IPv4					
1	VPN_A_Tunnel (Branch-HQ-A)	VPN_A_Tunnel (Branch-HQ-A)			0
2	VPN_B_Tunnel (Branch-HQ-B)	VPN_B_Tunnel (Branch-HQ-B)			0
3	HQ-MPLS (HQ-MPLS)	HQ-MPLS (HQ-MPLS)			0

3. Drag the selected policy route to the desired position.

<div> <div>+ Create New</div> <div>Edit</div> <div>Delete</div> <div>Search</div> <div>Q</div> </div>					
Seq.#	Incoming Interface	Outgoing Interface	Source	Destination	Hit Count
IPv4					
1	VPN_A_Tunnel (Branch-HQ-A)	VPN_A_Tunnel (Branch-HQ-A)			0
3	HQ-MPLS (HQ-MPLS)	HQ-MPLS (HQ-MPLS)			0
2	VPN_B_Tunnel (Branch-HQ-B)	VPN_B_Tunnel (Branch-HQ-B)			0

To move a policy route in the CLI:

```

config router policy
    move 3 after 1
end

```

Equal cost multi-path

Equal cost multi-path (ECMP) is a mechanism that allows a FortiGate to load-balance routed traffic over multiple gateways. Just like routes in a routing table, ECMP is considered after policy routing, so any matching policy routes will take precedence over ECMP.

ECMP pre-requisites are as follows:

- Routes must have the same destination and costs. In the case of static routes, costs include distance and priority
- Routes are sourced from the same routing protocol. Supported protocols include static routing, OSPF, and BGP

ECMP and SD-WAN implicit rule

ECMP and SD-WAN implicit rule are essentially similar in the sense that an SD-WAN implicit rule is processed after SD-WAN service rules are processed. See [Implicit rule on page 469](#) to learn more.

The following table summarizes the different load-balancing algorithms supported by each:

ECMP	SD-WAN		Description
	(GUI)	(CLI)	
source-ip-based	Source IP	source-ip-based	Traffic is divided equally between the interfaces. Sessions that start at the same source IP address use the same path. This is the default selection.
weight-based	Sessions	weight-based	The workload is distributed based on the number of sessions that are connected through the interface. The weight that you assign to each interface is used to calculate the percentage of the total sessions allowed to connect through an interface, and the sessions are distributed to the interfaces accordingly.
usage-based	Spillover	usage-based	The interface is used until the traffic bandwidth exceeds the ingress and egress thresholds that you set for that interface. Additional traffic is then sent through the next interface member.
source-dest-ip-based	Source-Destination IP	source-dest-ip-based	Traffic is divided equally between the interfaces. Sessions that start at the same source IP address and go to the same destination IP address use the same path.
Not supported	Volume	measured-volume-based	This mode is supported in SD-WAN only. The workload is distributed based on the number of packets that are going through the interface.

To configure the ECMP algorithm from the CLI:

- At the VDOM-level:


```
config system settings
    set v4-ecmp-mode {source-ip-based* | weight-based | usage-based | source-dest-ip-based}
end
```
- If SD-WAN is enabled, the above option is not available and ECMP is configured under the SD-WAN settings:


```
config system sdwan
    set sdwan enable
    set load-balance-mode {source-ip-based* | weight-based | usage-based | source-dest-ip-based | measured-volume-based}
end
```


For ECMP in IPv6, the mode must also be configured under SD-WAN.

```
# diagnose sys vd list
system fib version=63
list virtual firewall info:
name=root/root index=0 enabled fib_ver=40 use=168 rt_num=46 asym_rt=0 sip_helper=0, sip_nat_
  trace=1, mc_fwd=0, mc_ttl_nc=0, tpmc_sk_pl=0
ecmp=source-ip-based, ecmp6=source-ip-based asym_rt6=0 rt6_num=55 strict_src_check=0 dns_
  log=1 ses_num=20 ses6_num=0 pkt_num=19154477
```

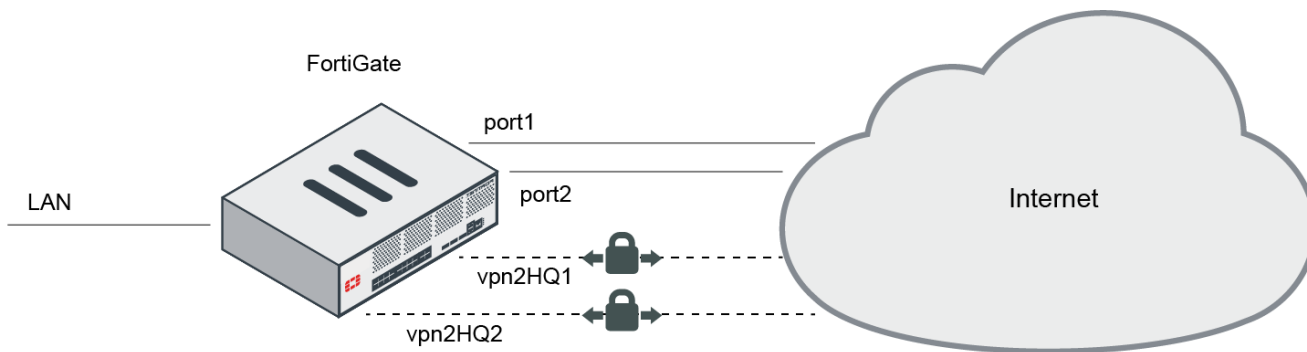
To change the number of paths allowed by ECMP:

```
config system settings
  set ecmp-max-paths <number of paths>
end
```



Setting `ecmp-max-paths` to the lowest value of 1 is equivalent to disabling ECMP.

ECMP configuration examples



The following examples demonstrate the behavior of ECMP in different scenarios:

- [Example 1: Default ECMP on page 419](#)
- [Example 2: Same distance, different priority on page 420](#)
- [Example 3: Weight-based ECMP on page 420](#)
- [Example 4: Load-balancing BGP routes on page 421](#)

Example 1: Default ECMP

```
config router static
  edit 1
    set gateway 172.16.151.1
    set device "port1"
  next
  edit 2
    set gateway 192.168.2.1
    set device "port2"
  next
end
```

```
# get router info routing-table all
Routing table for VRF=0
S*    0.0.0.0/0 [10/0] via 172.16.151.1, port1
      [10/0] via 192.168.2.1, port2
C     172.16.151.0/24 is directly connected, port1
C     192.168.2.0/24 is directly connected, port2
```

Result:

Both routes are added to the routing table and load-balanced based on the source IP.

Example 2: Same distance, different priority

```
config router static
  edit 1
    set gateway 172.16.151.1
    set priority 5
    set device "port1"
  next
  edit 2
    set gateway 192.168.2.1
    set device "port2"
  next
end

# get router info routing-table all
Routing table for VRF=0
S*    0.0.0.0/0 [10/0] via 192.168.2.1, port2
      [10/0] via 172.16.151.1, port1, [5/0]
C     172.16.151.0/24 is directly connected, port1
C     192.168.2.0/24 is directly connected, port2
```

Result:

Both routes are added to the routing table, but traffic is routed to `port2` which has a lower priority value with a default of 0.

Example 3: Weight-based ECMP

```
config router static
  edit 3
    set dst 10.10.30.0 255.255.255.0
    set weight 80
    set device "vpn2HQ1"
  next
  edit 5
    set dst 10.10.30.0 255.255.255.0
    set weight 20
    set device "vpn2HQ2"
  next
end

# get router info routing-table all
Routing table for VRF=0
...
```

```

S    10.10.30.0/24 [10/0] is directly connected, vpn2HQ1, [0/80]
      [10/0] is directly connected, vpn2HQ2, [0/20]
C    172.16.151.0/24 is directly connected, port1
C    192.168.0.0/24 is directly connected, port3
C    192.168.2.0/24 is directly connected, port2

```

Result:

Both routes are added to the routing table, but 80% of the sessions to 10.10.30.0/24 are routed to vpn2HQ1, and 20% are routed to vpn2HQ2.

Example 4: Load-balancing BGP routes

```

config router bgp
  set as 64511
  set router-id 192.168.2.86
  set ebgp-multipath enable
  config neighbor
    edit "192.168.2.84"
      set remote-as 64512
    next
    edit "192.168.2.87"
      set remote-as 64512
    next
  end
end

# get router info routing-table all
Routing table for VRF=0
...
C    172.16.151.0/24 is directly connected, port1
C    192.168.0.0/24 is directly connected, port3
C    192.168.2.0/24 is directly connected, port2
B    192.168.80.0/24 [20/0] via 192.168.2.84, port2, 00:00:33
      [20/0] via 192.168.2.87, port2, 00:00:33

```

Result:

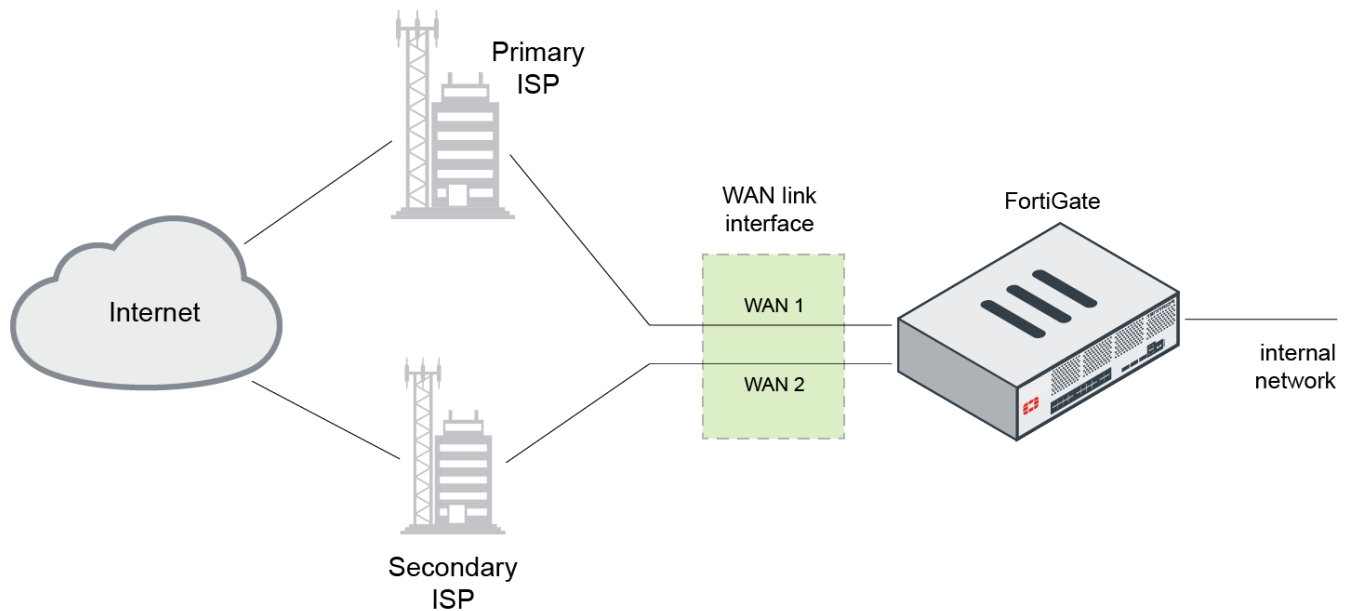
The network 192.168.80.0/24 is advertised by two BGP neighbors. Both routes are added to the routing table, and traffic is load-balanced based on Source IP.

For multiple BGP paths to be added to the routing table, you must enable `ebgp-multipath` for eBGP or `ibgp-multipath` for iBGP. These settings are disabled by default.

Dual internet connections

Dual internet connections, also referred to as dual WAN or redundant internet connections, refers to using two FortiGate interfaces to connect to the Internet. This is generally accomplished with SD-WAN, but this legacy solution provides the means to configure dual WAN without using SD-WAN. You can use dual internet connections in several ways:

- Link redundancy: If one interface goes down, the second interface automatically becomes the main connection.
- Load sharing: This ensures better throughput.
- Use a combination of link redundancy and load sharing.



This section describes the following dual internet connection scenarios:

- [Scenario 1: Link redundancy and no load-sharing on page 422](#)
- [Scenario 2: Load-sharing and no link redundancy on page 424](#)
- [Scenario 3: Link redundancy and load-sharing on page 426](#)

Scenario 1: Link redundancy and no load-sharing

Link redundancy ensures that if your Internet access is no longer available through a certain port, the FortiGate uses an alternate port to connect to the Internet.

In this scenario, two interfaces, WAN1 and WAN2, are connected to the Internet using two different ISPs. WAN1 is the primary connection. In the event of a failure of WAN1, WAN2 automatically becomes the connection to the Internet. For this configuration to function correctly, you must configure the following settings:

- [Link health monitor on page 422](#): To determine when the primary interface (WAN1) is down and when the connection returns.
- [Routing on page 423](#): Configure a default route for each interface.
- [Security policies on page 424](#): Configure security policies to allow traffic through each interface to the internal network.

Link health monitor

Adding a link health monitor is required for routing failover traffic. A link health monitor confirms the device interface connectivity by probing a gateway or server at regular intervals to ensure it is online and working. When the server is not accessible, that interface is marked as down.

Set the `interval` (how often to send a ping) and `failtime` (how many lost pings are considered a failure). A smaller interval value and smaller number of lost pings results in faster detection, but creates more traffic on your network.

The link health monitor supports both IPv4 and IPv6, and various other protocols including ping, tcp-echo, udp-echo, http, and twamp.

To add a link health monitor (IPv4) using the CLI:

```
config system link-monitor
  edit <link-monitor-name>
    set addr-mode ipv4
    set srcintf <interface-name>
    set server <server-IP-address>
    set protocol {ping tcp-echo udp-echo http twamp}
    set gateway-ip <gateway-IP-address>
    set interval <seconds>
    set failtime <retry-attempts>
    set recoverytime <number-of-successful-responses>
    set status enable
  next
end
```

Option	Description
set update-cascade-interface {enable disable}	This option is used in conjunction with fail-detect and fail-alert options in interface settings to cascade the link failure down to another interface. See the Bring other interfaces down when link monitor fails KB article for details.
set update-static-route {enable disable}	When the link fails, all static routes associated with the interface will be removed.

Routing

You must configure a default route for each interface and indicate your preferred route as follows:

- Specify different distances for the two routes. The lower of the two distance values is declared active and placed in the routing table

OR

- Specify the same distance for the two routes, but give a higher priority to the route you prefer by defining a lower value. Both routes will be added to the routing table, but the route with a higher priority will be chosen as the best route

In the following example, we will use the first method to configure different distances for the two routes. You might not be able to connect to the backup WAN interface because the FortiGate does not route traffic out of the backup interface. The FortiGate performs a reverse path look-up to prevent spoofed traffic. If an entry cannot be found in the routing table that sends the return traffic out through the same interface, the incoming traffic is dropped.

To configure the routing of the two interfaces using the GUI:

- Go to *Network > Static Routes*, and click *Create New*.
- Enter the following information:

Destination	For an IPv4 route, enter a subnet of 0.0.0.0/0.0.0.0. For an IPv6 route, enter a subnet of ::/0.
Interface	Select the primary connection. For example, wan1.

Gateway Address	Enter the gateway address.
Administrative Distance	Leave as the default of 10.

3. Click **OK**.

4. Repeat the above steps to set *Interface* to `wan2` and *Administrative Distance* to 20.

To configure the routing of the two interfaces using the CLI:

```
config router {static | static6}
edit 0
    set dst 0.0.0.0 0.0.0.0
    set device wan1
    set gateway <gateway_address>
    set distance 10
next
edit 0
    set dst 0.0.0.0 0.0.0.0
    set device wan2
    set gateway <gateway_address>
    set distance 20
next
end
```

Security policies

When you create security policies, you need to configure duplicate policies to ensure that after traffic fails over WAN1, regular traffic is allowed to pass through WAN2, as it did with WAN1. This ensures that failover occurs with minimal effect to users.

Scenario 2: Load-sharing and no link redundancy

Load sharing may be accomplished in a few of the following ways of the many possible ways:

- By defining a preferred route with a lower distance, and specifying policy routes to route certain traffic to the secondary interface.
- By defining routes with same distance values but different priorities, and specifying policy routes to route certain traffic to the secondary interface.
- By defining routes with same distance values and priorities, and use equal-cost multi-path (ECMP) routing to equally distribute traffic between the WAN interfaces.

In our example, we will use the first option for our configuration. In this scenario, because link redundancy is not required, you do not have to configure a link monitor.



Traffic behaviour without a link monitor is as follows:

- If the remote gateway is down but the primary WAN interface of a FortiGate is still up, the FortiGate will continue to route traffic to the primary WAN. This results in traffic interruptions.
- If the primary WAN interface of a FortiGate is down due to physical link issues, the FortiGate will remove routes to it and the secondary WAN routes will become active. Traffic will failover to the secondary WAN.

Routing

Configure routing as you did in [Scenario 1: Link redundancy and no load-sharing on page 422](#) above.

Policy routes

By configuring policy routes, you can redirect specific traffic to the secondary WAN interface. This works in this case because policy routes are checked before static routes. Therefore, even though the static route for the secondary WAN is not in the routing table, traffic can still be routed using the policy route.

In this example, we will create a policy route to route traffic from one address group to the secondary WAN interface.

To configure a policy route from the GUI:

1. Go to *Network > Policy Routes*, and click *Create New*.
2. Enter the following information:

Incoming interface	Define the source of the traffic. For example, <code>internal</code> .
Source Address	If we prefer to route traffic only from a group of addresses, define an address or address group, and add here.
Destination Address	Because we want to route all traffic from the address group here, we do not specify a destination address.
Protocol	Specify any protocol.
Action	Forward traffic.
Outgoing interface	Select the secondary WAN as the outbound interface. For example, <code>wan2</code> .
Gateway address	Input the gateway address for your secondary WAN. Because its default route has a higher distance value and is not added to the routing table, the gateway address must be added here.

3. Click OK.

To configure a policy route from the CLI:

```
config router policy
edit 1
    set input-device "internal"
    set srcaddr "Laptops"
    set gateway <gateway_address>
    set output-device "wan2"
next
end
```

Security policies

Your security policies should allow all traffic from `internal` to WAN1. Because link redundancy is not needed, you do not need to duplicate all WAN1 policies to WAN2. You will only need to define policies used in your policy route.

Scenario 3: Link redundancy and load-sharing

In this scenario, both the links are available to distribute Internet traffic with the primary WAN being preferred more. Should one of the interfaces fail, the FortiGate will continue to send traffic over the other active interface. The configuration is a combination of both the link redundancy and the load-sharing scenarios. The main difference is that the configured routes have equal distance values, with the route with a higher priority being preferred more. This ensures both routes are active in the routing table, but the route with a higher priority will be the best route.

Link health monitor

Link monitor must be configured for both the primary and the secondary WAN interfaces. This ensures that if the primary or the secondary WAN fails, the corresponding route is removed from the routing table and traffic re-routed to the other WAN interface.

For configuration details, see sample configurations in [Scenario 1: Link redundancy and no load-sharing on page 422](#).

Routing

Both WAN interfaces must have default routes with the same distance. However, preference is given to the primary WAN by giving it a higher priority.

To configure the routing of the two interfaces using the CLI:

```
config router {static | static6}
  edit 0
    set dst 0.0.0.0 0.0.0.0
    set device wan1
    set gateway <gateway_address>
    set distance 10
    set priority 0
  next
  edit 0
    set dst 0.0.0.0 0.0.0.0
    set device wan2
    set gateway <gateway_address>
    set distance 10
    set priority 10
  next
end
```

Policy routes

The policy routes configuration is very similar to that of the policy routes in [Scenario 2: Load-sharing and no link redundancy on page 424](#), except that the gateway address should not be specified. When a policy route is matched and the gateway address is not specified, the FortiGate looks at the routing table to obtain the gateway. In case the secondary WAN fails, traffic may hit the policy route. Because there is no gateway specified and the route to the secondary WAN is removed by the link monitor, the policy route will be bypassed and traffic will continue through the primary WAN. This ensures that the policy route is not active when the link is down.

Security policies

When you create security policies, you need to configure duplicate policies to ensure that after traffic fails over WAN1, regular traffic is allowed to pass through WAN2, as it was with WAN1. This ensures that failover occurs with minimal effect to users.

Multicast

The following topics include information about multicast:

- [Multicast routing and PIM support on page 427](#)
- [Configuring multicast forwarding on page 428](#)

Multicast routing and PIM support

Multicasting (also called IP multicasting) consists of using a single multicast source to send data to many receivers. Multicasting can be used to send data to many receivers simultaneously while conserving bandwidth and reducing network traffic. Multicasting can be used for one-way delivery of media streams to multiple receivers and for one-way data transmission for news feeds, financial information, and so on. Many dynamic routing protocols such as RIPv2, OSPF, and EIGRP use multicasting to share hello packets and routing information.

A FortiGate can operate as a Protocol Independent Multicast (PIM) version 2 router. FortiGates support PIM sparse mode ([RFC 4601](#)) and PIM dense mode ([RFC 3973](#)), and can service multicast servers or receivers on the network segment to which a FortiGate interface is connected. Multicast routing is not supported in transparent mode.

To support PIM communications, the sending and receiving applications, and all connecting PIM routers in between, must be enabled with PIM version 2. PIM can use static routes, RIP, OSPF, or BGP to forward multicast packets to their destinations. To enable source-to-destination packet delivery, sparse mode or dense mode must be enabled on the PIM router interfaces. Sparse mode routers cannot send multicast messages to dense mode routers. If the FortiGate is located between a source and a PIM router, between two PIM routers, or is connected directly to a receiver, you must manually create a multicast policy to pass encapsulated (multicast) packets or decapsulated data (IP traffic) between the source and destination.

PIM domains

A PIM domain is a logical area comprising a number of contiguous networks. The domain contains at least one bootstrap router (BSR), and if sparse mode is enabled, a number of rendezvous points (RPs) and designated routers (DRs). When PIM is enabled, the FortiGate can perform any of these functions at any time as configured.

A PIM domain can be configured in the GUI by going to *Network > Multicast*, or in the CLI using `config router multicast`. Note that PIM version 2 must be enabled on all participating routers between the source and receivers. Use `config router multicast` to set the global operating parameters.

When PIM is enabled, the FortiGate allocates memory to manage mapping information. The FortiGate communicates with neighboring PIM routers to acquire mapping information and, if required, processes the multicast traffic associated with specific multicast groups.

Instead of sending multiple copies of generated IP traffic to more than one specific IP destination address, PIM-enabled routers encapsulate the data and use a Class D multicast group address (224.0.0.0 to 239.255.255.255) to forward

multicast packets to multiple destinations. A single stream of data can be sent because one destination address is used. Client applications receive multicast data by requesting that the traffic destined for a certain multicast group address be delivered to them.

Configuring multicast forwarding

There is sometimes confusion between the terms forwarding and routing. These two functions should not take place at the same time. Multicast forwarding should be enabled when the FortiGate is in NAT mode and you want to forward multicast packets between multicast routers and receivers. However, this function should not be enabled when the FortiGate itself is operating as a multicast router, or has an applicable routing protocol that uses multicast.

There are two steps to configure multicast forwarding:

1. [Enable multicast forwarding](#)
2. [Configure multicast policies](#)

Enabling multicast forwarding

Multicast forwarding is enabled by default. If a FortiGate is operating in transparent mode, adding a multicast policy enables multicast forwarding. In NAT mode you must use the `multicast-forward` setting to enable or disable multicast forwarding.

Multicast forwarding in NAT mode

When `multicast-forward` is enabled, the FortiGate forwards any multicast IP packets in which the TTL is 2 or higher to all interfaces and VLAN interfaces, except the receiving interface. The TTL in the IP header will be reduced by 1. Even though the multicast packets are forwarded to all interfaces, you must add multicast policies to allow multicast packets through the FortiGate.

To enable multicast forwarding in NAT mode:

```
config system settings
    set multicast-forward enable
end
```

Prevent the TTL for forwarded packets from being changed

You can use the `multicast-ttl-notchange` option so that the FortiGate does not increase the TTL value for forwarded multicast packets. Use this option only if packets are expiring before reaching the multicast router.

To prevent the TTL for forwarded packets from being changed:

```
config system settings
    set multicast-ttl-notchange enable
end
```

Disable multicast traffic from passing through the FortiGate without a policy check in transparent mode

In transparent mode, the FortiGate does not forward frames with multicast destination addresses. The FortiGate should not interfere with the multicast traffic used by routing protocols, streaming media, or other multicast communication. To avoid any issues during transmission, you can disable `multicast-skip-policy` and configure multicast security policies.

To disable multicast traffic from passing through the FortiGate without a policy check in transparent mode:

```
config system settings
    set multicast-skip-policy disable
end
```

Configuring multicast policies

Multicast packets require multicast policies to allow packets to pass from one interface to another. Similar to firewall policies, in a multicast policy you specify the source and destination interfaces, and the allowed address ranges for the source and destination addresses of the packets. You can also use multicast policies to configure source NAT and destination NAT for multicast packets.

Keep the following in mind when configuring multicast policies:

- The matched forwarded (outgoing) IP multicast source IP address is changed to the configured IP address.
- The `snat` setting is optional. Use it when SNAT is needed.

Sample basic policy

In this basic policy, multicast packets received on an interface are flooded unconditionally to all interfaces on the forwarding domain, except the incoming interface.

```
config firewall multicast-policy
    edit 1
        set srcintf "any"
        set dstintf "any"
        set srcaddr "all"
        set dstaddr "all"
    next
end
```

The destination address (`dstaddr`) is a multicast address object. The `all` option corresponds to all multicast addresses in the range 224.0.0.0-239.255.255.255.

Sample policy with specific source and destination interfaces

This multicast policy only applies to the source port `wan1` and the destination port `internal`.

```
config firewall multicast-policy
    edit 1
        set srcintf "wan1"
        set dstintf "internal"
        set srcaddr "all"
        set dstaddr "all"
    next
end
```

```
    next
end
```

Sample policy with specific source address object

In this policy, packets are allowed to flow from `wan1` to `internal`, and sourced by the address 172.20.120.129, which is represented by the `example_addr-1` address object.

```
config firewall multicast-policy
    edit 1
        set srcintf "wan1"
        set dstintf "internal"
        set srcaddr "example_addr-1"
        set dstaddr "all"
    next
end
```

Sample detailed policy

This policy accepts multicast packets that are sent from a PC with IP address 192.168.5.18 to destination address range 239.168.4.0-255. The policy allows the multicast packets to enter the `internal` interface and then exit the `external` interface. When the packets leave the external interface, their source address is translated to 192.168.18.10.

```
config firewall address
    edit "192.168.5.18"
        set subnet 192.168.5.18 255.255.255.255
    next
end

config firewall multicast-address
    edit "239.168.4.0"
        set start-ip 239.168.4.0
        set end-ip 239.168.4.255
    next
end

config firewall multicast-policy
    edit 1
        set srcintf "internal"
        set dstintf "external"
        set srcaddr "192.168.5.18"
        set dstaddr "239.168.4.0"
        set snat enable
        set snat-ip 192.168.18.10
    next
end
```



To configure multicast policies in the GUI, enable *Multicast Policy* in *System > Feature Visibility*.

Direct IP support for LTE/4G

Direct IP is a public IP address that is assigned to a computing device, which allows the device to directly access the internet.

When an LTE modem is enabled in FortiOS, a DHCP interface is created. As a result, the FortiGate can acquire direct IP (which includes IP, DNS, and gateway) from the LTE network carrier.

Since some LTE modems require users to input the access point name (APN) for the LTE network, the LTE modem configuration allows you to set the APN.



LTE modems can only be enabled by using the CLI.

To enable direct IP support using the CLI:

1. Enable the LTE modem:

```
config system lte-modem
    set status enable
end
```

2. Check that the LTE interface was created:

```
config system interface
    edit "wwan"
        set vdom "root"
        set mode dhcp
        set status down
        set distance 1
        set type physical
        set snmp-index 23
    next
end
```

Shortly after the LTE modem joins its carrier network, `wwan` is enabled and granted direct IP:

```
# config system interface
(interface) # edit wwan
(wwan) # get
name                : wwan
....
ip                  : 100.112.75.43 255.255.255.248
....
status              : up
....
defaultgw           : enable
DHCP Gateway        : 100.112.75.41
Lease Expires       : Thu Feb 21 19:33:27 2019
dns-server-override : enable
Acquired DNS1       : 184.151.118.254
Acquired DNS2       : 70.28.245.227
....
```

PCs can reach the internet via the following firewall policy:

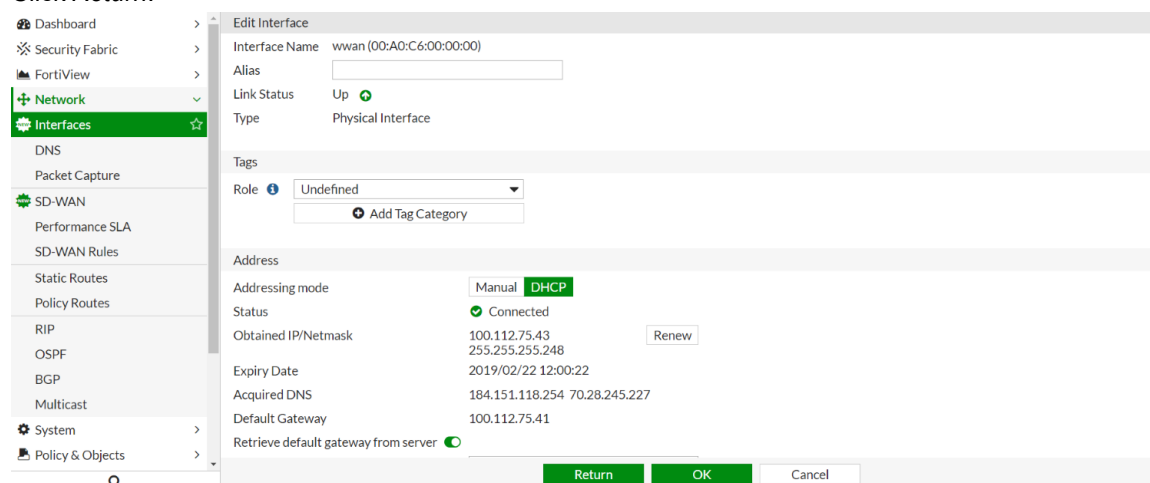
```
config firewall policy
....
edit 5
    set name "LTE"
    set uuid 61880e9a-36ce-51e9-a4f4-15cc3ffc25f3
    set srcintf "port9"
    set dstintf "wwan"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set fsso disable
    set nat enable
next
end
```

Sample LTE interface

When an LTE modem is enabled, you can view the LTE interface in the GUI and check the acquired IP, DNS, and gateway.

To view the LTE interface in the GUI:

1. Go to *Network > Interfaces*.
2. Double-click the LTE interface to view the properties.
3. Look in the *Address* section to view the:
 - a. *Obtained IP*
 - b. *Acquired DNS*
 - c. *Default Gateway*
4. Click *Return*.



To configure the firewall policy that uses the LTE interface:

1. Go to *Policy & Objects > IPv4 Policy*.
2. Double-click the LTE policy. The *Edit Policy* pane opens.
3. In the *Outgoing Interface* field, select the interface (*wwan* in this example).
4. Configure the rest of the policy as needed.

The screenshot displays the FortiGate GUI's 'Edit Policy' window. On the left, a sidebar contains a tree view with categories like Dashboard, Security Fabric, FortiView, Network, System, and Policy & Objects. Under 'Policy & Objects', 'IPv4 Policy' is selected. The main area is titled 'Edit Policy' and contains several configuration sections. The top section has fields for Name (LTE), Incoming Interface (port9), Outgoing Interface (wwan), Source (all), Destination (all), Schedule (always), and Service (ALL). The Action section shows 'ACCEPT' selected, with 'DENY' and 'LEARN' as options. Below this is the 'Firewall / Network Options' section, which includes NAT (enabled), IP Pool Configuration (Use Outgoing Interface Address), Preserve Source Port (disabled), and Protocol Options (PRX default). The bottom section, 'Security Profiles', shows AntiVirus and Web Filter both disabled.

5. Click **OK**.

Limitations

- Most LTE modems have a preset APN in their SIM card. Therefore, the APN does not need to be set in the FortiOS configuration. In cases where the internet cannot be accessed, consult with your carrier and set the APN in the LTE modem configuration (for example, inet.bell.ca):

```
config system lte-modem
  set status enable
  set apn "inet.bell.ca"
end
```

- Some models, such as the FortiGate 30E-3G4G, have built-in LTE modems. In this scenario, the LTE modem is enabled by default. The firewall policy via the LTE interface is also created by default. Once you plug in a SIM card, your network devices can connect to the internet.

Sample FortiGate 30E-3G4G default configuration:

```
config system lte-modem
  set status enable
  set extra-init ''
  set manual-handover disable
  set force-wireless-profile 0
  set authtype none
  set apn ''
  set modem-port 255
end
```

```
    set network-type auto
    set auto-connect disable
    set gpsd-enabled disable
    set data-usage-tracking disable
    set gps-port 255
end

config firewall policy
....
edit 3
    set uuid f7c77cc6-36d1-51e9-2899-a7040791330c
    set srcintf "internal"
    set dstintf "wan"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set nat enable
next
end
```

LLDP reception

Natively, device detection can scan LLDP as a source for device identification. However, the FortiGate does not read or store the full information. Enabling LLDP reception allows the FortiGate to receive and store LLDP messages, learn about active neighbors, and makes the LLDP information available via the CLI, REST API, and SNMP.

You will need to enable `device-identification` at the interface level, and then `lldp-reception` can be enabled on three levels: globally, per VDOM, or per interface.

To configure device identification on an interface:

```
config system interface
    edit <port>
        set device-identification enable
    next
end
```

To configure LLDP reception globally:

```
config system global
    set lldp-reception enable
end
```

To configure LLDP reception per VDOM:

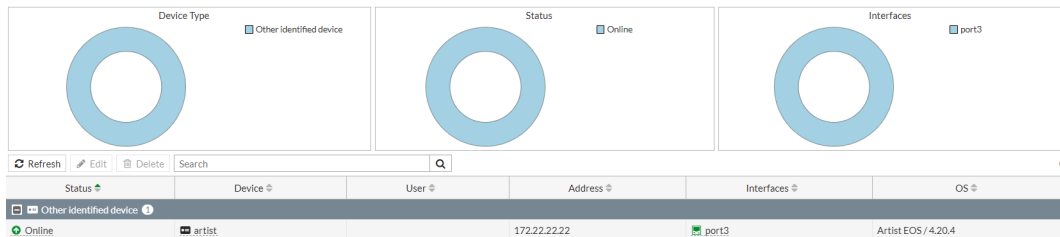
```
config system setting
    set lldp-reception enable
end
```


To configure LLDP reception per interface:

```
config system interface
  edit <port>
    set lldp-reception enable
  next
end
```

To view the LLDP information in the GUI:

1. Go to *User & Device > Device Inventory* to view the information.

**To view the received LLDP information in the CLI:**

```
# diagnose user device list
hosts
  vd root/0 44:0a:a0:0a:0a:0a gen 3 req S/2
  created 10290s gen 1 seen 0s port3 gen 1
  ip 172.22.22.22 src lldp
  type 20 'Other Network Device' src lldp id 155 gen 2
  os 'Artist EOS ' version '4.20.4' src lldp id 155
  host 'artist' src lldp
```

To view additional information about LLDP neighbors and ports:

```
# diagnose lldprx neighbor {summary | details | clear}
# diagnose lldprx port {details | summary | neighbor | filter}
# diagnose lldprx port neighbor {summary | details}
```

Note that the port index in the output corresponds to the port index from the following command:

```
# diagnose netlink interface list port2 port3 | grep index
if=port2 family=00 type=1 index=4 mtu=1500 link=0 master=0
if=port3 family=00 type=1 index=5 mtu=1500 link=0 master=0
```

To view the received LLDP information in the REST API:

```
{
  "http_method": "GET",
  "results": [
    {
      "mac": "90:9c:9c:c9:c9:90",
      "chassis_id": "90:9C:9C:C9:C9:90",
      "port": 19,
      "port_id": "port12",
      "port_desc": "port12",
    }
  ]
}
```

```
    "system_name": "S124DN3W000000000",
    "system_desc": "FortiSwitch-124D v3.6.6, build0416, 180515 (GA)",
    "ttl": 120,
    "addresses": [
      {
        "type": "ipv4",
        "address": "192.168.1.99"
      }
    ]
  },
  "vdom": "root",
  "path": "network",
  "name": "lldp",
  "action": "neighbors",
  "status": "success",
  "serial": "FG201E4Q000000000",
  "version": "v6.2.0",
  "build": 866
}

{
  "http_method": "GET",
  "results": [
    {
      "name": "port1",
      "rx": 320,
      "neighbors": 1
    }
  ],
  "vdom": "root",
  "path": "network",
  "name": "lldp",
  "action": "ports",
  "mkey": "port1",
  "status": "success",
  "serial": "FG201E4Q000000000",
  "version": "v6.2.0",
  "build": 866
}
```

NetFlow

NetFlow allows you to collect IP network traffic statistics for an interface, and then export those statistics for analysis. NetFlow samplers, that sample every packet, are configured per interface. Full NetFlow is supported through the information maintained in the firewall session.

To configure NetFlow:

```
config system netflow
  set collector-ip <ip>
  set collector-port <port>
  set source-ip <ip>
```

```

    set active-flow-timeout <integer>
    set inactive-flow-timeout <integer>
    set template-tx-timeout <integer>
    set template-tx-counter <integer>
end

```

collector-ip <ip>	Collector IP address.
collector-port <port>	NetFlow collector port number (0 - 65535)
source-ip <ip>	Source IP address, for communication with the NetFlow agent.
active-flow-timeout <integer>	Timeout to report active flows, in minutes (1 - 60, default = 30).
inactive-flow-timeout <integer>	Timeout for periodic report of finished flows, in seconds (10 - 600, default = 15).
template-tx-timeout <integer>	Timeout for periodic template flowset transmission, in minutes (1 - 1440, default = 30).
template-tx-counter <integer>	Counter of flowset records, before resending a template flowset record (10 - 6000, default = 20).

To configure NetFlow in a specific VDOM:

```

config vdom
    edit <vdom>
        config system vdom-netflow
            set vdom-netflow enable
            set collector-ip <ip>
            set collector-port <port>
            set source-ip <ip>
        end
    end
next
end

```

To configure a NetFlow sampler on an interface:

```

config system interface
    edit <interface>
        set netflow-sampler {disable | tx | rx | both}
    next
end

```

disable	Disable the NetFlow protocol on this interface (default).
tx	Monitor transmitted traffic on this interface.
rx	Monitor received traffic on this interface.
both	Monitor transmitted/received traffic on this interface.

Verification and troubleshooting

If data are not seen on the NetFlow collector after it has been configured, use the following sniffer commands to verify if the FortiGate and the collector are communicating:

- By collector port:

```
# diagnose sniffer packet 'port <collector-port>' 6 0 a
```

- By collector IP address:

```
# diagnose sniffer packet 'host <collector-ip>' 6 0 a
```

NetFlow uses the sflow daemon. The current NetFlow configuration can be viewed using test level 3 or 4:

```
# diagnose test application sflowd 3
```

```
# diagnose test application sflowd 4
```

Netflow Cache Stats:

```
vdoms=1 Collectors=1 Cached_intf=2 Netflow_enabled_intf=1 Live_sessions=0 Session cache max count:71950
```

NetFlow templates

Netflow uses templates to capture and categorize the data that it collects. FortiOS supports the following Netflow templates:

Name	Template ID	Description
STAT_OPTIONS	256	Statistics information about exporter
APP_ID_OPTIONS	257	Application information
IPV4	258	No NAT IPv4 traffic
IPV6	259	No NAT IPv6 traffic
ICMP4	260	No NAT ICMPv4 traffic
ICMP6	261	No NAT ICMPv6 traffic
IPV4_NAT	262	Source/Destination NAT IPv4 traffic
IPV4_AF_NAT	263	AF NAT IPv4 traffic (4->6)
IPV6_NAT	264	Source/Destination NAT IPv6 traffic
IPV6_AF_NAT	265	AF NAT IPv6 traffic (6->4)
ICMP4_NAT	266	Source/Destination NAT ICMPv4 traffic
ICMP4_AF_NAT	267	AF NAT ICMPv4 traffic (4->6)
ICMP6_NAT	268	Source/Destination NAT ICMPv6 traffic
ICMPv6_AF_NAT	269	AF NAT ICMPv6 traffic (6->4)

256 - STAT_OPTIONS

Description	Statistics information about exporter
Scope Field Count	1
Data Field Count	7
Option Scope Length	4
Option Length	28
Padding	0000

Scope fields

Field #	Field	Type	Length
1	System	System (1)	2

Data fields

Field #	Field	Type	Length
1	TOTAL_BYTES_EXP	TOTAL_BYTES_EXP (40)	8
2	TOTAL_PKTS_EXP	TOTAL_PKTS_EXP (41)	8
3	TOTAL_FLOWS_EXP	TOTAL_FLOWS_EXP (42)	8
4	FLOW_ACTIVE_TIMEOUT	FLOW_ACTIVE_TIMEOUT (36)	2
5	FLOW_INACTIVE_TIMEOUT	FLOW_INACTIVE_TIMEOUT (37)	2
6	SAMPLING_INTERVAL	SAMPLING_INTERVAL (34)	4
7	SAMPLING_ALGORITHM	SAMPLING_ALGORITHM (35)	1

257 - APP_ID_OPTIONS

Description	Application information
Scope Field Count	1
Data Field Count	4
Option Scope Length	4
Option Length	16
Padding	0000

Scope fields

Field #	Field	Type	Length
1	System	System (1)	2

Data fields

Field #	Field	Type	Length
1	APPLICATION_ID	APPLICATION_ID (95)	9
2	APPLICATION_NAME	APPLICATION_NAME (96)	64
3	APPLICATION_DESC	APPLICATION_DESC (94)	64
4	applicationCategoryName	applicationCategoryName (372)	32

258 - IPV4

Description	No NAT IPv4 traffic
Data Field Count	17

Data fields

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	L4_SRC_PORT	L4_SRC_PORT (7)	2
8	L4_DST_PORT	L4_DST_PORT (11)	2
9	INPUT_SNMP	INPUT_SNMP (10)	2
10	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
11	PROTOCOL	PROTOCOL (4)	1
12	APPLICATION_ID	APPLICATION_ID (95)	9
13	FLOW_FLAGS	FLOW_FLAGS (65)	2
14	FORWARDING_STATUS	FORWARDING_STATUS (89)	1

Field #	Field	Type	Length
15	flowEndReason	flowEndReason (136)	1
16	IP_SRC_ADDR	IP_SRC_ADDR (8)	4
17	IP_DST_ADDR	IP_DST_ADDR (12)	4

259 - IPV6

Description	No NAT IPv6 traffic
Data Field Count	17

Data fields

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	L4_SRC_PORT	L4_SRC_PORT (7)	2
8	L4_DST_PORT	L4_DST_PORT (11)	2
9	INPUT_SNMP	INPUT_SNMP (10)	2
10	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
11	PROTOCOL	PROTOCOL (4)	1
12	APPLICATION_ID	APPLICATION_ID (95)	9
13	FLOW_FLAGS	FLOW_FLAGS (65)	2
14	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
15	flowEndReason	flowEndReason (136)	1
16	IPV6_SRC_ADDR	IPV6_SRC_ADDR (27)	16
17	IPV6_DST_ADDR	IPV6_DST_ADDR (28)	16

260 - ICMP4

Description	No NAT ICMPv4 traffic
Data Field Count	16

Data fields

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	INPUT_SNMP	INPUT_SNMP (10)	2
8	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
9	ICMP_TYPE	ICMP_TYPE (32)	2
10	PROTOCOL	PROTOCOL (4)	1
11	APPLICATION_ID	APPLICATION_ID (95)	9
12	FLOW_FLAGS	FLOW_FLAGS (65)	2
13	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
14	flowEndReason	flowEndReason (136)	1
15	IP_SRC_ADDR	IP_SRC_ADDR (8)	4
16	IP_DST_ADDR	IP_DST_ADDR(12)	4

261 - ICMP6

Description	No NAT ICMPv6 traffic
Data Field Count	16

Data fields

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4

Field #	Field	Type	Length
7	INPUT_SNMP	INPUT_SNMP (10)	2
8	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
9	ICMP_TYPE	ICMP_TYPE (32)	2
10	PROTOCOL	PROTOCOL (4)	1
11	APPLICATION_ID	APPLICATION_ID (95)	9
12	FLOW_FLAGS	FLOW_FLAGS (65)	2
13	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
14	flowEndReason	flowEndReason (136)	1
15	IPv6_SRC_ADDR	IPv6_SRC_ADDR (27)	16
16	IPv6_DST_ADDR	IPv6_DST_ADDR (28)	16

262 - IPV4_NAT

Description	Source/Destination NAT IPv4 traffic
Data Field Count	21

Data fields

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	L4_SRC_PORT	L4_SRC_PORT (7)	2
8	L4_DST_PORT	L4_DST_PORT (11)	2
9	INPUT_SNMP	INPUT_SNMP (10)	2
10	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
11	PROTOCOL	PROTOCOL (4)	1
12	APPLICATION_ID	APPLICATION_ID (95)	9
13	FLOW_FLAGS	FLOW_FLAGS (65)	2

Field #	Field	Type	Length
14	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
15	flowEndReason	flowEndReason (136)	1
16	IP_SRC_ADDR	IP_SRC_ADDR (8)	4
17	IP_DST_ADDR	IP_DST_ADDR (12)	4
18	postNATSourceIPv4Address	postNATSourceIPv4Address (225)	4
19	postNATDestinationIPv4Address	postNATDestinationIPv4Address (226)	4
20	postNAPTSourceTransportPort	postNAPTSourceTransportPort (227)	2
21	postNAPTDestinationTransportPort	postNAPTDestinationTransportPort (228)	2

263 - IPV4_AF_NAT

Description	AF NAT IPv4 traffic (4->6)
Data Field Count	21

Data fields

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	L4_SRC_PORT	L4_SRC_PORT (7)	2
8	L4_DST_PORT	L4_DST_PORT (11)	2
9	INPUT_SNMP	INPUT_SNMP (10)	2
10	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
11	PROTOCOL	PROTOCOL (4)	1
12	APPLICATION_ID	APPLICATION_ID (95)	9
13	FLOW_FLAGS	FLOW_FLAGS (65)	2
14	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
15	flowEndReason	flowEndReason (136)	1

Field #	Field	Type	Length
16	IPV6_SRC_ADDR	IPV6_SRC_ADDR (27)	16
17	IPV6_DST_ADDR	IPV6_DST_ADDR (28)	16
18	postNATSourceIPv6Address	postNATSourceIPv6Address (281)	16
19	postNATDestinationIPv6Address	postNATDestinationIPv6Address (282)	16
20	postNAPTSourceTransportPort	postNAPTSourceTransportPort (227)	2
21	postNAPTDestinationTransportPort	postNAPTDestinationTransportPort (228)	2

264 - IPV6_NAT

Description	Source/Destination NAT IPv6 traffic
Data Field Count	21

Data fields

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	L4_SRC_PORT	L4_SRC_PORT (7)	2
8	L4_DST_PORT	L4_DST_PORT (11)	2
9	INPUT_SNMP	INPUT_SNMP (10)	2
10	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
11	PROTOCOL	PROTOCOL (4)	1
12	APPLICATION_ID	APPLICATION_ID (95)	9
13	FLOW_FLAGS	FLOW_FLAGS (65)	2
14	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
15	flowEndReason	flowEndReason (136)	1
16	IP_SRC_ADDR	IP_SRC_ADDR (8)	4
17	IP_DST_ADDR	IP_DST_ADDR (12)	4

Field #	Field	Type	Length
18	postNATSourceIPv6Address	postNATSourceIPv6Address (281)	16
19	postNATDestinationIPv6Address	postNATDestinationIPv6Address (282)	16
20	postNAPTSourceTransportPort	postNAPTSourceTransportPort (227)	2
21	postNAPTDestinationTransportPort	postNAPTDestinationTransportPort (228)	2

265 - IPV6_AF_NAT

Description	AF NAT IPv6 traffic (6->4)
Data Field Count	21

Data fields

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	L4_SRC_PORT	L4_SRC_PORT (7)	2
8	L4_DST_PORT	L4_DST_PORT (11)	2
9	INPUT_SNMP	INPUT_SNMP (10)	2
10	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
11	PROTOCOL	PROTOCOL (4)	1
12	APPLICATION_ID	APPLICATION_ID (95)	9
13	FLOW_FLAGS	FLOW_FLAGS (65)	2
14	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
15	flowEndReason	flowEndReason (136)	1
16	IPV6_SRC_ADDR	IPV6_SRC_ADDR (27)	16
17	IPV6_DST_ADDR	IPV6_DST_ADDR (28)	16
18	postNATSourceIPv4Address	postNATSourceIPv4Address (225)	4
19	postNATDestinationIPv4Address	postNATDestinationIPv4Address (226)	4

Field #	Field	Type	Length
20	postNAPTSourceTransportPort	postNAPTSourceTransportPort (227)	2
21	postNAPTDestinationTransportPort	postNAPTDestinationTransportPort (228)	2

266 - ICMPV4_NAT

Description	Source/Destination NAT ICMPv4 traffic
Data Field Count	20

Data fields

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	INPUT_SNMP	INPUT_SNMP (10)	2
8	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
9	ICMP_TYPE	ICMP_TYPE (32)	2
10	PROTOCOL	PROTOCOL (4)	1
11	APPLICATION_ID	APPLICATION_ID (95)	9
12	FLOW_FLAGS	FLOW_FLAGS (65)	2
13	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
14	flowEndReason	flowEndReason (136)	1
15	IP_SRC_ADDR	IP_SRC_ADDR (8)	4
16	IP_DST_ADDR	IP_DST_ADDR (12)	4
17	postNATSourceIPv4Address	postNATSourceIPv4Address (225)	4
18	postNATDestinationIPv4Address	postNATDestinationIPv4Address (226)	4
19	postNAPTSourceTransportPort	postNAPTSourceTransportPort (227)	2
20	postNAPTDestinationTransportPort	postNAPTDestinationTransportPort (228)	2

267 - ICMPV4_AF_NAT

Description	AF NAT ICMPv4 traffic (4->6)
Data Field Count	20

Data fields

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	INPUT_SNMP	INPUT_SNMP (10)	2
8	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
9	ICMP_TYPE	ICMP_TYPE (32)	2
10	PROTOCOL	PROTOCOL (4)	1
11	APPLICATION_ID	APPLICATION_ID (95)	9
12	FLOW_FLAGS	FLOW_FLAGS (65)	2
13	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
14	flowEndReason	flowEndReason (136)	1
15	IPV6_SRC_ADDR	IPV6_SRC_ADDR (27)	16
16	IPV6_DST_ADDR	IPV6_DST_ADDR (28)	16
17	postNATSourceIPv6Address	postNATSourceIPv6Address (281)	16
18	postNATDestinationIPv6Address	postNATDestinationIPv6Address (282)	16
19	postNAPTSourceTransportPort	postNAPTSourceTransportPort (227)	2
20	postNAPTDestinationTransportPort	postNAPTDestinationTransportPort (228)	2

268 - ICMPV6_NAT

Description	Source/Destination NAT ICMPv6 traffic
Data Field Count	20

Data fields

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	INPUT_SNMP	INPUT_SNMP (10)	2
8	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
9	ICMP_TYPE	ICMP_TYPE (32)	2
10	PROTOCOL	PROTOCOL (4)	1
11	APPLICATION_ID	APPLICATION_ID (95)	9
12	FLOW_FLAGS	FLOW_FLAGS (65)	2
13	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
14	flowEndReason	flowEndReason (136)	1
15	IP_SRC_ADDR	IP_SRC_ADDR (8)	4
16	IP_DST_ADDR	IP_DST_ADDR (12)	4
17	postNATSourceIPv6Address	postNATSourceIPv6Address (281)	16
18	postNATDestinationIPv6Address	postNATDestinationIPv6Address (282)	16
19	postNAPTSourceTransportPort	postNAPTSourceTransportPort (227)	2
20	postNAPTDestinationTransportPort	postNAPTDestinationTransportPort (228)	2

269 - ICMPV6_AF_NAT

Description	AF NAT ICMPv6 traffic (6->4)
Data Field Count	20

Data fields

Field #	Field	Type	Length
1	BYTES	BYTES (1)	8

Field #	Field	Type	Length
2	OUT_BYTES	OUT_BYTES (23)	8
3	PKTS	PKTS (2)	4
4	OUT_PKTS	OUT_PKTS (24)	4
5	FIRST_SWITCHED	FIRST_SWITCHED (22)	4
6	LAST_SWITCHED	LAST_SWITCHED (21)	4
7	INPUT_SNMP	INPUT_SNMP (10)	2
8	OUTPUT_SNMP	OUTPUT_SNMP (14)	2
9	ICMP_TYPE	ICMP_TYPE (32)	2
10	PROTOCOL	PROTOCOL (4)	1
11	APPLICATION_ID	APPLICATION_ID (95)	9
12	FLOW_FLAGS	FLOW_FLAGS (65)	2
13	FORWARDING_STATUS	FORWARDING_STATUS (89)	1
14	flowEndReason	flowEndReason (136)	1
15	IPV6_SRC_ADDR	IPV6_SRC_ADDR (27)	16
16	IPV6_DST_ADDR	IPV6_DST_ADDR (28)	16
17	postNATSourceIPv4Address	postNATSourceIPv4Address (225)	4
18	postNATDestinationIPv4Address	postNATDestinationIPv4Address (226)	4
19	postNAPTSourceTransportPort	postNAPTSourceTransportPort (227)	2
20	postNAPTDestinationTransportPort	postNAPTDestinationTransportPort (228)	2

SD-WAN

SD-WAN is a software-defined approach to managing Wide-Area Networks (WAN). It allows you to offload internet-bound traffic, meaning that private WAN services remain available for real-time and mission critical applications. This added flexibility improves traffic flow and reduces pressure on the network.

SD-WAN platforms create hybrid networks that integrate broadband and other network services into the corporate WAN while maintaining the performance and security of real-time and sensitive applications.

SD-WAN with Application Aware Routing can measure and monitor the performance of multiple services in a hybrid network. It uses application routing to offer more granular control of where and when an application uses a specific service, allowing better use of the overall network.

Some of the key benefits of SD-WAN include:

- Reduced cost with transport independence across MPLS, 3G/4G LTE, and others.
- Improve business application performance thanks to increased availability and agility.
- Optimized user experience and efficiency with SaaS and public cloud applications.

SD-WAN has 3 objects:

- **SD-WAN interface**

Also called members, SD-WAN interfaces are the ports and interfaces that are used to run traffic. At least one interface must be configured for SD-WAN to function; up to 255 member interfaces can be configured. See [Configuring the SD-WAN interface on page 452](#).

- **Performance SLA**

Also called health-check, performance SLAs are used to monitor member interface link quality, and to detect link failures. They can be used to remove routes, and to reroute traffic when an SD-WAN member cannot detect the server. They can also be used in SD-WAN rules to select the preferred member interface for forwarding traffic. See [Performance SLA - link monitoring on page 463](#).

- **SD-WAN rule**

Also called service, SD-WAN rules are used to control path selection. Specific traffic can be dynamically sent to the best link, or use a specific route. There are five modes:

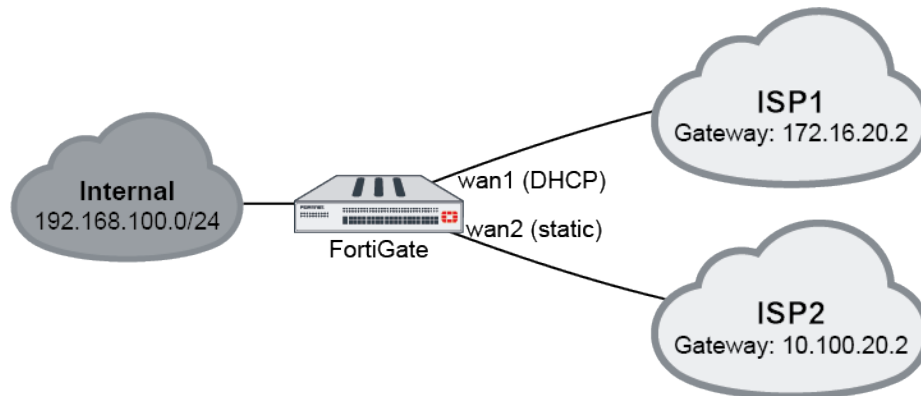
- *auto*: Assign interfaces a priority based on quality.
- *manual*: Assign interfaces a priority manually.
- *priority*: Assign interfaces a priority based on the link-cost-factor quality of the interface.
- *sla*: Assign interfaces a priority based on selected SLA settings.
- *load-balance*: Distribute traffic among all available links based on the load balance algorithm.

See [SD-WAN rules - best quality on page 472](#), [SD-WAN rules - lowest cost \(SLA\) on page 475](#), and [SD-WAN rules - maximize bandwidth \(SLA\) on page 477](#).

SD-WAN quick start

This section provides an example of how to start using SD-WAN for load balancing and redundancy.

In this example, two ISP internet connections, wan1 (DHCP) and wan2 (static), use SD-WAN to balance traffic between them at 50% each.



1. [Configuring the SD-WAN interface on page 452](#)
2. [Adding a static route on page 454](#)
3. [Selecting the implicit SD-WAN algorithm on page 454](#)
4. [Configuring security policies for SD-WAN on page 455](#)
5. [Link monitoring and failover on page 455](#)
6. [Results on page 457](#)
7. [Configuring SD-WAN in the CLI on page 461](#)

Configuring the SD-WAN interface

First, SD-WAN must be enabled and member interfaces must be selected. The selected FortiGate interfaces can be of any type (physical, aggregate, VLAN, IPsec, and others), but must be removed from any other configurations on the FortiGate.

In this step, two interfaces are configured and then selected as SD-WAN member interfaces. This example uses a mix of static and dynamic IP addresses; your deployment could also use only one or the other.

Once the SD-WAN interface is configured, it is referenced as *SD-WAN* in the GUI for static routes and firewall policies, and `virtual-wan-link` can be enabled in the CLI.

To configure SD-WAN members:

1. Configure the wan1 and wan2 interfaces. See [Interface settings on page 316](#) for details.
 - a. Set the wan1 interface *Addressing mode* to *DHCP* and *Distance* to *10*.



By default, a DHCP interface has a distance of 5, and a static route has a distance of 10. It is important to account for this when configuring your SD-WAN for 50/50 load balancing by setting the DHCP interface's distance to 10.

- b. Set the wan2 interface *IP/Netmask* to *10.100.20.1 255.255.255.0*.
2. Go to *Network > SD-WAN* and set *Status* to *Enable*.
Routing for each SD-WAN interface is defined here.

3. In the *SD-WAN Interface Members* table, click *Create New*.

SD-WAN New SD-WAN Member

Name SD-WAN

Type SD-WAN Interface

Status Enable Disable

Interface

Gateway 0.0.0.0

Cost 0

OK Cancel

4. Select *wan1* as the interface.
5. As wan1 uses DHCP, leave *Gateway* as the default *0.0.0.0*.
If IPv6 visibility is enabled in the GUI, an IPv6 gateway can also be added for each member. See [Feature visibility on page 732](#) for details.
6. Leave *Cost* as *0*.
The *Cost* field is used by the Lowest Cost (SLA) strategy. The link with the lowest cost is chosen to pass traffic. The lowest possible *Cost* is *0*.
7. Set *Status* to *Enable*, and click *OK*.
8. Repeat the above steps for wan2, setting *Gateway* to the ISP's gateway: *10.100.20.2*.
9. Click *Apply*.

SD-WAN

Name SD-WAN

Type SD-WAN Interface

Status Enable Disable

SD-WAN Interface Members

Interfaces	Gateway	Cost
to_ISP1 (wan1)	0.0.0.0	0
to_ISP2 (wan2)	10.100.20.2	0

SD-WAN Usage

Bandwidth Volume Sessions

Upstream

wan1: 0 bps
wan2: 0 bps

50% 50%

Downstream

wan1: 3.2 kbps
wan2: 3.2 kbps

50% 50%

Apply

SD-WAN Usage shows pie charts of usage per interface member.

Adding a static route

After you create an SD-WAN interface, FortiGate adds a virtual interface for SD-WAN to the interface list that can be used to create routes.

You must configure a default route for the SD-WAN interface. The default gateways for each SD-WAN member interface do not need to be defined in the static routes table. FortiGate will decide which route or routes are preferred using Equal Cost Multi-Path (ECMP) based on distance and priority.

To create a static route for SD-WAN:

1. Go to *Network > Static Routes*.
2. Click *Create New*. The *New Static Route* page opens.
3. Set *Destination* to *Subnet*, and leave the IP address and subnet mask as *0.0.0.0/0.0.0.0*.
4. From the *Interface* drop-down list, select *SD-WAN*.

The screenshot shows the 'New Static Route' configuration window. It includes the following fields and options:

- Dynamic Gateway:** A toggle switch that is currently turned off.
- Destination:** A dropdown menu set to 'Subnet' with a text input field containing '0.0.0.0/0.0.0.0'.
- Interface:** A dropdown menu set to 'SD-WAN'.
- Administrative Distance:** A text input field containing '10'.
- Comments:** A text input field with the placeholder 'Write a comment...' and a character count '0/255'.
- Status:** Two radio buttons, 'Enabled' (selected) and 'Disabled'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

5. Ensure that *Status* is *Enabled*.
6. Click *OK* to save your changes.

Selecting the implicit SD-WAN algorithm

SD-WAN rules define specific routing options to route traffic to an SD-WAN member.

If no routing rules are defined, the default *Implicit* rule is used. It can be configured to use one of five different load balancing algorithms. See [Implicit rule on page 469](#) for more details and examples.

This example shows four methods to equally balance traffic between the two WAN connections. Go to *Network > SD-WAN Rules* and edit the *sd-wan* rule to select the method that is appropriate for your requirements.

- **Source IP** (CLI command: `source-ip-based`):
Select this option to balance traffic equally between the SD-WAN members according to a hash algorithm based on the source IP addresses.
- **Session** (weight-based):
Select this option to balance traffic equally between the SD-WAN members by the session numbers ratio among its members. Use weight 50 for each of the 2 members.
- **Source-Destination IP** (source-dest-ip-based):
Select this option to balance traffic equally between the SD-WAN members according to a hash algorithm based on the source and destination IP addresses.
- **Volume** (measured-volume-based):
Select this option to balance traffic equally between the SD-WAN members according to the bandwidth ratio among its members.

Configuring security policies for SD-WAN

After you create an SD-WAN interface, FortiGate adds a virtual interface for SD-WAN to the interface list that can be used to create security policies.

You must configure a policy that allows traffic from your organization's internal network to the SD-WAN interface (`virtual-wan-link` in the CLI). You do not need to configure policies for each individual SD-WAN member interface because policies configured with the SD-WAN interface apply to all SD-WAN interface members.

To create a security policy for SD-WAN:

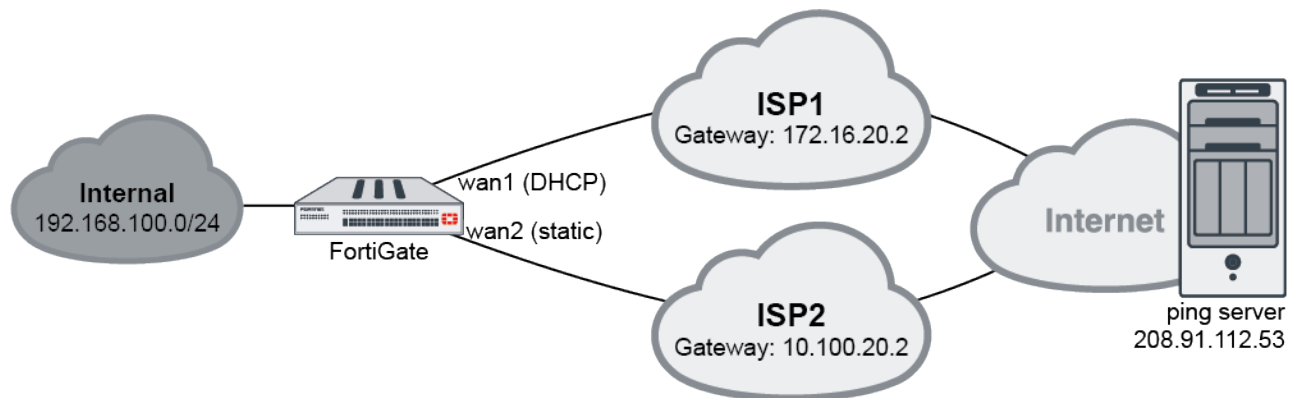
1. Go to *Policy & Objects > IPv4 Policy*.
2. Click *Create New*. The *New Policy* page opens.
3. Configure the following:

Name	Enter a name for the policy.
Incoming Interface	<i>internal</i>
Outgoing Interface	<i>SD-WAN</i>
Source	<i>all</i>
Destination	<i>all</i>
Schedule	<i>always</i>
Service	<i>ALL</i>
Action	<i>ACCEPT</i>
Firewall / Network Options	Enable <i>NAT</i> and set <i>IP Pool Configuration</i> to <i>Use Outgoing Interface Address</i> .
Security Profiles	Apply profiles as required.
Logging Options	Enable <i>Log Allowed Traffic</i> and select <i>All Sessions</i> . This allows you to verify results later.

4. Enable the policy, then click *OK*.

Link monitoring and failover

Performance SLA link monitoring measures the health of links that are connected to SD-WAN member interfaces by sending probing signals through each link to a server, and then measuring the link quality based on latency, jitter, and packet loss. If a link is broken, the routes on that link are removed and traffic is routed through other links. When the link is working again, the routes are re-enabled. This prevents traffic being sent to a broken link and lost.



In this example, the detection server IP address is 208.91.112.53. A performance SLA is created so that, if ping fails per the metrics defined, the routes to that interface are removed and traffic is detoured to the other interface. The ping protocol is used, but other protocols could also be selected as required.

To configure a performance SLA:

1. Go to *Network > Performance SLA*.
2. Click *Create New*. The *Performance SLA* page opens.
3. Enter a name for the SLA and select a protocol.
4. In the *Server* field, enter the detection server IP address (208.91.112.53 in this example).
5. In the *Participants* field, select both wan1 and wan2.

New Performance SLA

Name: server

Protocol: **Ping** HTTP

Server: 208.91.112.53

Participants: to_ISP1 (wan1), to_ISP2 (wan2)

Enable probe packets: ☒

SLA Targets: [Add Target](#)

Link Status

Check interval: 500 ms

Failures before inactive: 5

Restore link after: 5 check(s)

Actions when Inactive

Update static route: ☒

OK Cancel

SLA targets are not required for link monitoring.

6. Configure the required metrics in *Link Status*.
7. Ensure that *Update static route* is enabled. This disables static routes for the inactive interface and restores routes on recovery.
8. Click *OK*.

Results

The following GUI pages show the function of the SD-WAN and can be used to confirm that it is setup and running correctly:

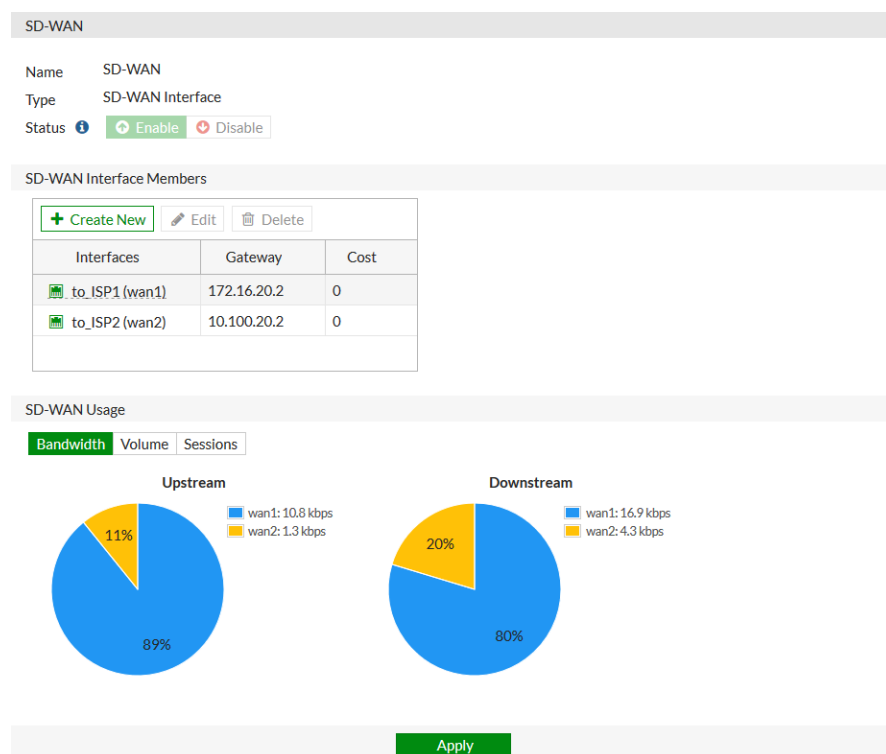
- [Interface usage on page 457](#)
- [Routing table on page 460](#)
- [Interface monitor on page 460](#)
- [Firewall policy on page 461](#)

Interface usage

Go to *Network > SD-WAN* to review the SD-WAN interfaces' statuses.

Bandwidth

Select *Bandwidth* to view the amount of downloaded and uploaded data for each interface.



Volume

Select *Volume* to see pie charts of the received and sent bytes on the interfaces.

SD-WAN

Name SD-WAN

Type SD-WAN Interface

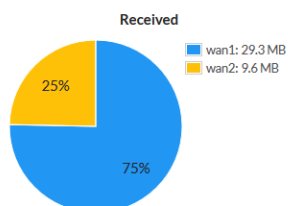
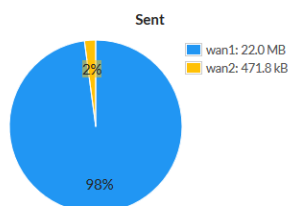
Status Enable Disable

SD-WAN Interface Members

Create New	Edit	Delete
Interfaces	Gateway	Cost
to_ISP1 (wan1)	172.16.20.2	0
to_ISP2 (wan2)	10.100.20.2	0

SD-WAN Usage

Bandwidth **Volume** Sessions



Apply

Sessions

Select **Sessions** to see a pie chart of the number of active sessions on each interface.

SD-WAN

Name SD-WAN
Type SD-WAN Interface
Status Enable Disable

SD-WAN Interface Members

Interfaces	Gateway	Cost
to_ISP1 (wan1)	172.16.20.2	0
to_ISP2 (wan2)	10.100.20.2	0

SD-WAN Usage

Bandwidth Volume **Sessions**

Sessions

wan1: 4
wan2: 5

Apply

Performance SLA

Go to **Network > Performance SLA** and select the SLA from the table (**server** in this example) to view the packet loss, latency, and jitter on each SD-WAN member in the health check server.

Packet loss

Select **Packet Loss** to see the percentage of packets lost for each member.

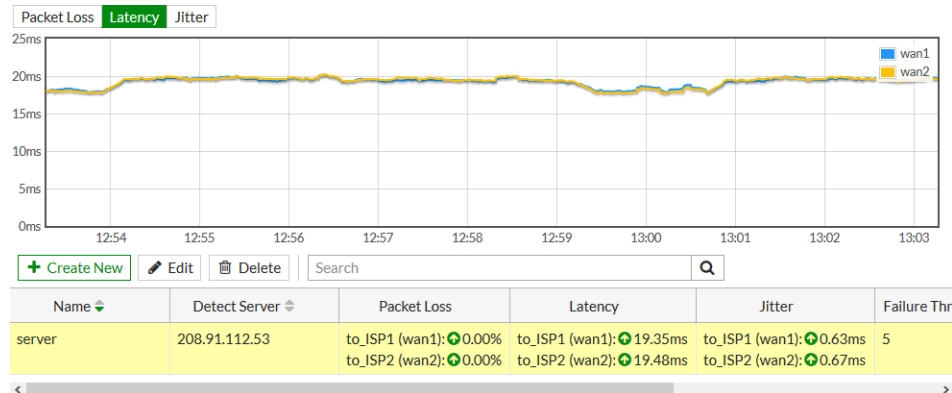
Packet Loss Latency Jitter

Create New Edit Delete

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Thresh
server	208.91.112.53	to_ISP1 (wan1): 0.00% to_ISP2 (wan2): 0.00%	to_ISP1 (wan1): 17.86ms to_ISP2 (wan2): 17.87ms	to_ISP1 (wan1): 0.72ms to_ISP2 (wan2): 0.54ms	5

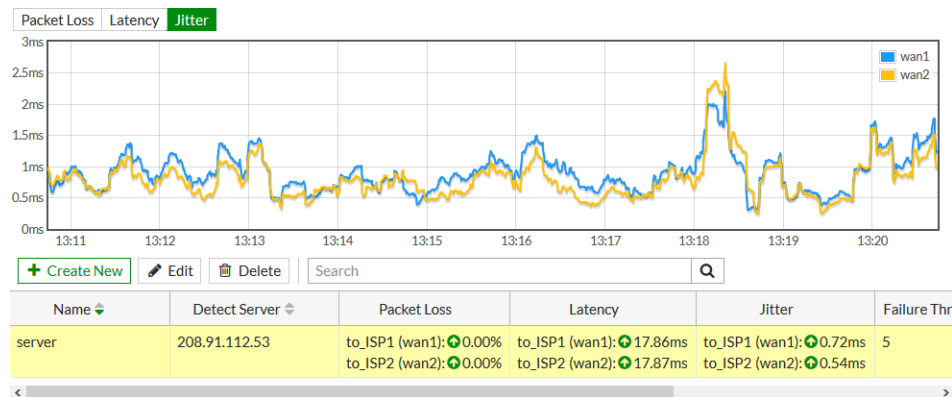
Latency

Select *Latency* to see the current latency, in milliseconds, for each member.



Jitter

Select *Jitter* to see the jitter, in milliseconds, for each member.



Routing table

Go to *Monitor > Routing Monitor* and to review all static and dynamic routes.

Refresh Route Lookup View Create Address Search Static & Dynamic Policy

Type	Network	Gateway IP	Interfaces	Distance
Static	0.0.0.0/0	172.16.20.2	to_ISP1 (wan1)	1
Static	0.0.0.0/0	10.100.20.2	to_ISP2 (wan2)	1
Connected	192.168.0.0/24	0.0.0.0	internal (port1)	0
Connected	192.168.0.0/24	0.0.0.0	port2	0
Connected	192.168.0.0/24	0.0.0.0	port3	0

Interface monitor

Go to *Monitor > SD-WAN Monitor* to review interface status, sessions, and usage.

[Refresh](#)

Interface	Status	Sessions	Upload	Download
sd-wan 4				
wan1		2	36.26 kbps	29.76 kbps
wan2		4	1.71 kbps	5.21 kbps

Firewall policy

Go to *Policy & Objects > IPv4 Policy* to review the SD-WAN policy.

[+ Create New](#) [Edit](#) [Delete](#) [Policy Lookup](#) Search [Interface Pair View](#) By Sequence IPv4 + IPv6

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
sd-wan 1									
sd-wan	all	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	All	2.63 GB
Implicit 1									
Implicit Deny	all	all	always	ALL	DENY			Disabled	3 MB

Configuring SD-WAN in the CLI

This example can be entirely configured using the CLI.

To configure SD-WAN in the CLI:

1. Configure the wan1 and wan2 interfaces:

```
config system interface
    edit "wan1"
        set alias to_ISP1
        set mode dhcp
        set distance 10
    next
    edit "wan2"
        set alias to_ISP2
        set ip 10.100.20.1 255.255.255.0
    next
end
```

2. Enable SD-WAN and add the interfaces as members:

```
config system virtual-wan-link
    set status enable
    config members
        edit 1
            set interface "wan1"
        next
        edit 2
            set interface "wan2"
            set gateway 10.100.20.2
        next
    end
end
```

3. Create a static route for SD-WAN:

```
config router static
  edit 1
    set virtual-wan-link enable
  next
end
```

4. Select the implicit SD-WAN algorithm:

```
config system virtual-wan-link
  set load-balance-mode {source-ip-based | weight-based | source-dest-ip-based |
measured-volume-based}
end
```

5. Create a firewall policy for SD-WAN:

```
config firewall policy
  edit <policy_id>
    set name <policy_name>
    set srcintf internal
    set dstintf virtual-wan-link
    set srcaddr all
    set dstaddr all
    set action accept
    set schedule always
    set service ALL
    set utm-status enable
    set ssl-ssh-profile <profile_name>
    set av-profile <profile_name>
    set webfilter-profile <profile_name>
    set dnsfilter-profile <profile_name>
    set application-list <app_list>
    set logtraffic all
    set nat enable
    set status enable
  next
end
```

6. Configure a performance SLA:

```
config system virtual-wan-link
  config health-check
    edit "server"
      set server "208.91.112.53"
      set update-static-route enable
      set members 1 2
    next
  end
end
```

Results

To view the routing table in the CLI:

```
# get router info routing-table all

Routing table for VRF=0
```

```

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [1/0] via 172.16.20.2, wan1
         [1/0] via 10.100.20.2, wan2
C       10.100.20.0/24 is directly connected, wan2
C       172.16.20.2/24 is directly connected, wan1
C       192.168.0.0/24 is directly connected, internal

```

To diagnose the Performance SLA status:

```

FGT # diagnose sys virtual-wan-link health-check
Health Check(server):
Seq(1): state(alive), packet-loss(0.000%) latency(15.247), jitter(5.231) sla_map=0x0
Seq(2): state(alive), packet-loss(0.000%) latency(13.621), jitter(6.905) sla_map=0x0

```

WAN path control

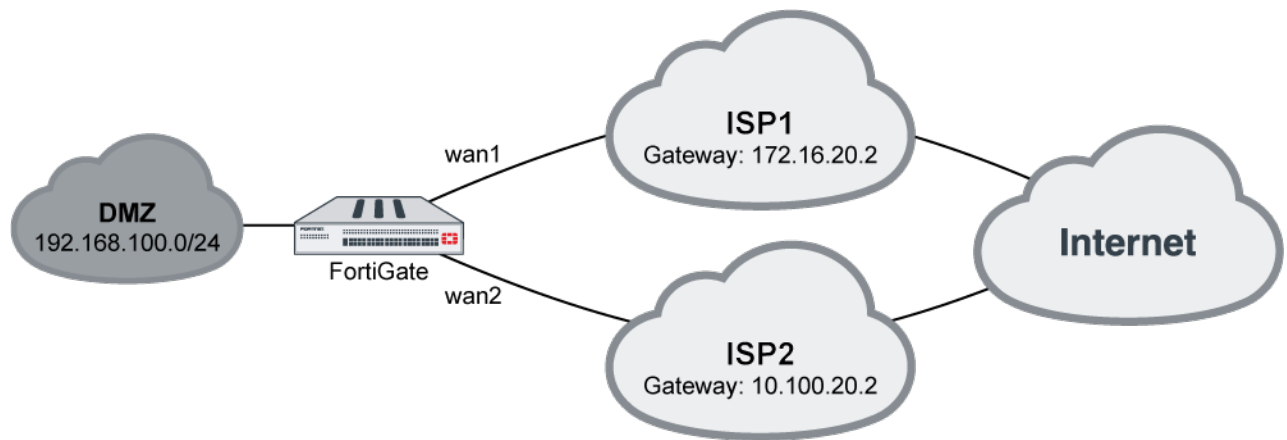
The following topics provide instructions on configuring WAN path control:

- [Performance SLA - link monitoring on page 463](#)
- [Performance SLA - SLA targets on page 465](#)
- [Factory default health checks on page 466](#)
- [Implicit rule on page 469](#)
- [SD-WAN rules - best quality on page 472](#)
- [SD-WAN rules - lowest cost \(SLA\) on page 475](#)
- [SD-WAN rules - maximize bandwidth \(SLA\) on page 477](#)
- [Application steering using SD-WAN rules on page 480](#)
- [SD-WAN traffic shaping and QoS on page 492](#)
- [Per-link controls for policies and SLA checks on page 496](#)
- [DSCP tag-based traffic steering in SD-WAN on page 498](#)

Performance SLA - link monitoring

Performance SLA link health monitoring measures the health of links that are connected to SD-WAN member interfaces by sending probing signals through each link to a server and measuring the link quality based on latency, jitter, and packet loss. If a link fails all of the health checks, the routes on that link are removed from the SD-WAN link load balancing group, and traffic is routed through other links. When the link is working again the routes are reestablished. This prevents traffic being sent to a broken link and lost.

When an SD-WAN member has multiple health checks configured, all of the checks must fail for the routes on that link to be removed from the SD-WAN link load balancing group.



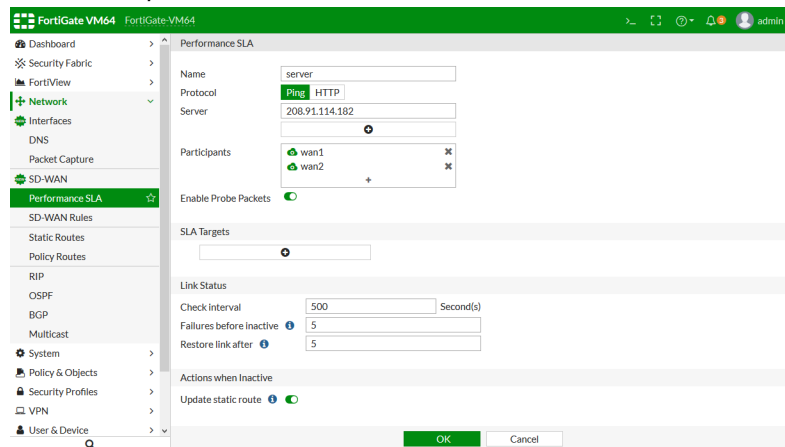
In this example:

- Interfaces wan1 and wan2 connect to the internet through separate ISPs
- The detection server IP address is 208.91.114.182

A performance SLA is created so that, if one link fails, its routes are removed and traffic is detoured to the other link.

To configure a Performance SLA using the GUI:

1. On the FortiGate, enable SD-WAN and add wan1 and wan2 as SD-WAN members, then add a policy and static route. See [Configuring the SD-WAN interface on page 452](#) for details.
2. Go to *Network > Performance SLA*.
3. Click *Create New*. The *Performance SLA* page opens.
4. Enter a name for the SLA and select a protocol.
5. In the *Server* field, enter the detection server IP address (208.91.114.182 in this example).
6. In the *Participants* field, select both wan1 and wan2.



7. Configured the remaining settings as needed, then click *OK*.

To configure a Performance SLA using the CLI:

```

config system virtual-wan-link
    config health-check
        edit "server"
            set server "208.91.114.182"
        end
    end
end

```

```

        set update-static-route enable
        set members 1 2
    next
end
end
end

```

To diagnose the Performance SLA status:

```

FGT # diagnose sys virtual-wan-link health-check
Health Check(server):
Seq(1): state(alive), packet-loss(0.000%) latency(15.247), jitter(5.231) sla_map=0x0
Seq(2): state(alive), packet-loss(0.000%) latency(13.621), jitter(6.905) sla_map=0x0

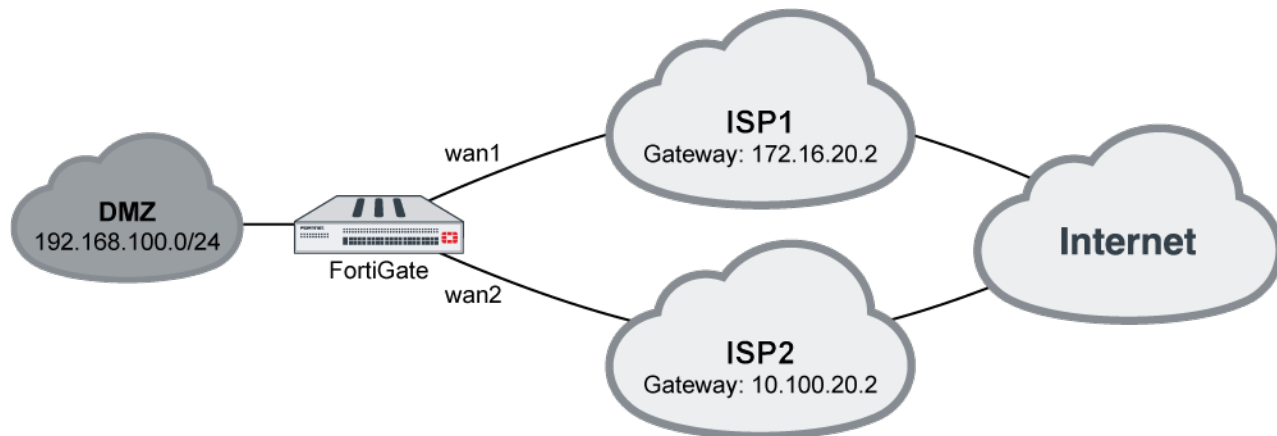
```

Performance SLA - SLA targets

SLA targets are a set of constraints that are used in SD-WAN rules to control the paths that traffic take.

The available constraints are:

- *Latency threshold*: Latency for SLA to make decision, in milliseconds (0 - 10000000, default = 5).
- *Jitter threshold*: Jitter for SLA to make decision, in milliseconds (0 - 10000000, default = 5).
- *Packet loss threshold*: Packet loss for SLA to make decision, in percentage (0 - 100, default = 0).



To configure Performance SLA targets using the GUI:

1. On the FortiGate, enable SD-WAN and add wan1 and wan2 as SD-WAN members, then add a policy and static route. See [Configuring the SD-WAN interface on page 452](#) for details.
2. Go to *Network > Performance SLA*.
3. Create a new Performance SLA or edit an existing one. See [Performance SLA - link monitoring on page 463](#).
4. Under *SLA Targets*, click the plus icon to add a target.

5. Turn on or off the required constraints, and set their values.

6. Configured the remaining settings as needed, then click **OK**.

To configure Performance SLA targets using the GUI:

```
config system virtual-wan-link
  config health-check
    edit "server"
      set server "208.91.114.182"
      set members 1 2
    config sla
      edit 1
        set link-cost-factor latency jitter packet-loss
        set latency-threshold 10
        set jitter-threshold 10
        set packetloss-threshold 1
      next
    end
  next
end
```

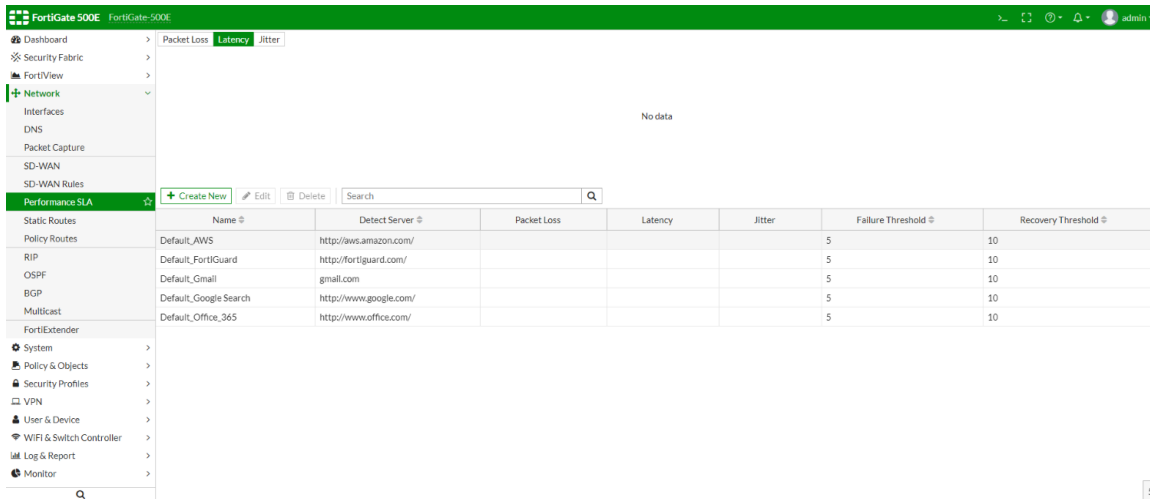
The `link-cost-factor` variable is used to select which constraints are enabled.

Factory default health checks

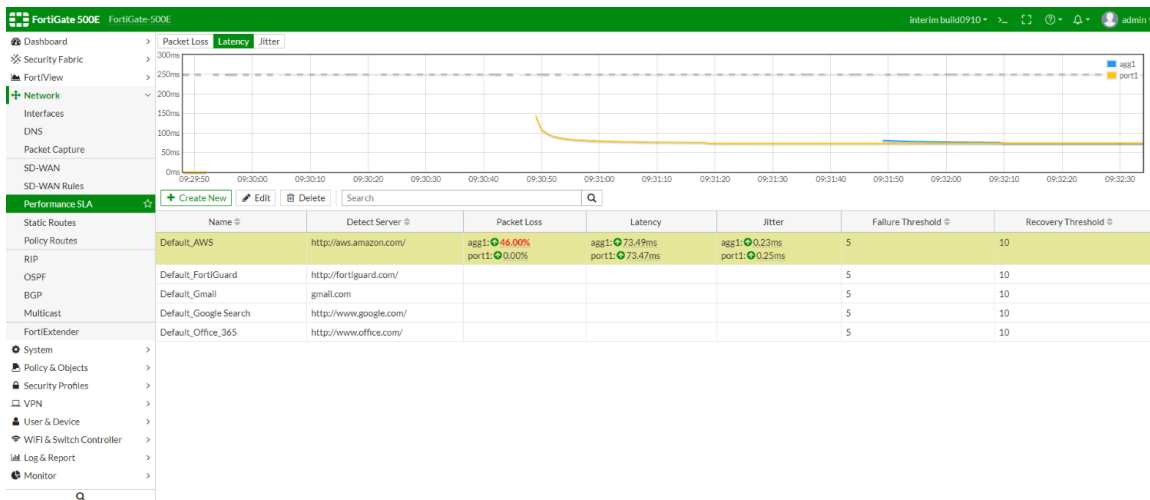
There are five predefined performance SLA profiles for newly created VDOMs or factory reset FortiGate devices:

- AWS
- FortiGuard
- Gmail
- Google Search
- Office 365

You can view and configure the SLA profiles in *Network > Performance SLA*.



After configuring a health check, you will be able to view packet loss, latency, and jitter data for the SLA profiles. If a value is colored red, it means that it failed to meet the SLA requirements.



To configure the performance SLA profiles in the CLI:

```
config system virtual-wan-link
  config health-check
    edit "Default_Office_365"
      set server "www.office.com"
      set protocol http
      set interval 1000
      set recoverytime 10
    config sla
      edit 1
        set latency-threshold 250
        set jitter-threshold 50
        set packetloss-threshold 5
      next
    end
  next
  edit "Default_Gmail"
```

```
        set server "gmail.com"
        set interval 1000
        set recoverytime 10
        config sla
            edit 1
                set latency-threshold 250
                set jitter-threshold 50
                set packetloss-threshold 2
            next
        end
    next
edit "Default_AWS"
    set server "aws.amazon.com"
    set protocol http
    set interval 1000
    set recoverytime 10
    config sla
        edit 1
            set latency-threshold 250
            set jitter-threshold 50
            set packetloss-threshold 5
        next
    end
next
edit "Default_Google Search"
    set server "www.google.com"
    set protocol http
    set interval 1000
    set recoverytime 10
    config sla
        edit 1
            set latency-threshold 250
            set jitter-threshold 50
            set packetloss-threshold 5
        next
    end
next
edit "Default_FortiGuard"
    set server "fortiguard.com"
    set protocol http
    set interval 1000
    set recoverytime 10
    config sla
        edit 1
            set latency-threshold 250
            set jitter-threshold 50
            set packetloss-threshold 5
        next
    end
next
end
end
```

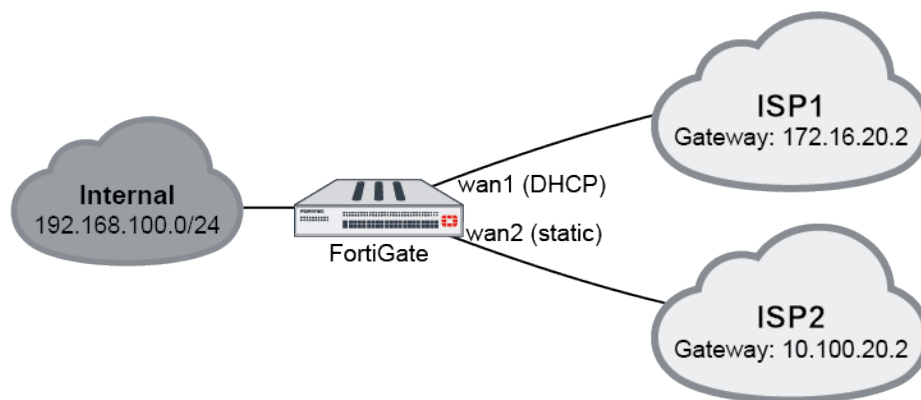
Implicit rule

SD-WAN supports five types of implicit rules (load-balance mode):

- Source IP (CLI command: `source-ip-based`): SD-WAN will load balance the traffic equally among its members according to a hash algorithm based on the source IP addresses.
- Session (`weight-based`): SD-WAN will load balance the traffic according to the session numbers ratio among its members.
- Spillover (`usage-based`): SD-WAN will use the first member until the bandwidth reaches its limit, then use the second, and so on.
- Source-Destination IP (`source-dest-ip-based`): SD-WAN will load balance the traffic equally among its members according to a hash algorithm based on both the source and destination IP addresses.
- Volume (`measured-volume-based`): SD-WAN will load balance the traffic according to the bandwidth ratio among its members.

Examples

The following four examples demonstrate how to use the implicit rules (load-balance mode).



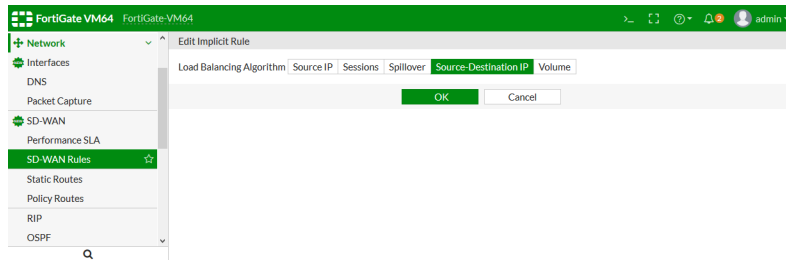
Example 1

Outgoing traffic is equally balanced between wan1 and wan2, using *source-ip-based* or *source-dest-ip-based* mode.

Using the GUI:

1. On the FortiGate, enable SD-WAN and add wan1 and wan2 as SD-WAN members, then add a policy and static route. See [Configuring the SD-WAN interface on page 452](#) for details.
2. Go to *Network > SD-WAN Rules*.
3. Edit the *sd-wan* rule (the last default rule).

- For the *Load Balancing Algorithm*, select either *Source IP* or *Source-Destination IP*.



- Click **OK**.

Using the CLI:

- Enable SD-WAN and add wan1 and wan2 as SD-WAN members, then add a policy and static route. See [Configuring the SD-WAN interface on page 452](#) for details.
- Set the load balancing algorithm:
Source IP based:

```
config system virtual-wan-link
    set load-balance-mode source-ip-based
end
```

Source-Destination IP based:

```
config system virtual-wan-link
    set load-balance-mode source-dest-ip-based
end
```

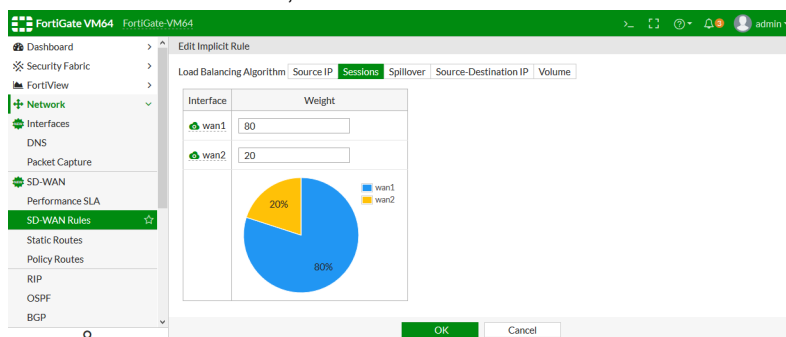
Example 2

Outgoing traffic is balanced between wan1 and wan2 with a customized ratio, using *weight-based* mode: wan1 runs 80% of the sessions, and wan2 runs 20% of the sessions.

Sessions with the same source and destination IP addresses (`src-ip` and `dst-ip`) will be forwarded to the same path, but will still be considered in later session ratio calculations.

Using the GUI:

- Go to *Network > SD-WAN Rules*.
- Edit the *sd-wan* rule (the last default rule).
- For the *Load Balancing Algorithm*, select *Sessions*.
- Enter 80 in the *wan1* field, and 20 in the *wan2* field.



5. Click *OK*.

Using the CLI:

```
config system virtual-wan-link
  set load-balance-mode weight-based
  config members
    edit 1
      set interface "wan1"
      set weight 80
    next
    edit 2
      set interface "wan2"
      set weight 20
    next
  end
end
```

Example 3

Outgoing traffic is balanced between wan1 and wan2 with a customized ratio, using *measured-volume-based* mode: wan1 runs 80% of the volume, and wan2 runs 20% of the volume.

Using the GUI:

1. Go to *Network > SD-WAN Rules*.
2. Edit the *sd-wan* rule (the last default rule).
3. For the *Load Balancing Algorithm*, select *Volume*.
4. Enter 80 in the *wan1* field, and 20 in the *wan2* field.
5. Click *OK*.

Using the CLI:

```
config system virtual-wan-link
  set load-balance-mode measured-volume-based
  config members
    edit 1
      set interface "wan1"
      set volume-ratio 80
    next
    edit 2
      set interface "wan2"
      set volume-ratio 20
    next
  end
end
```

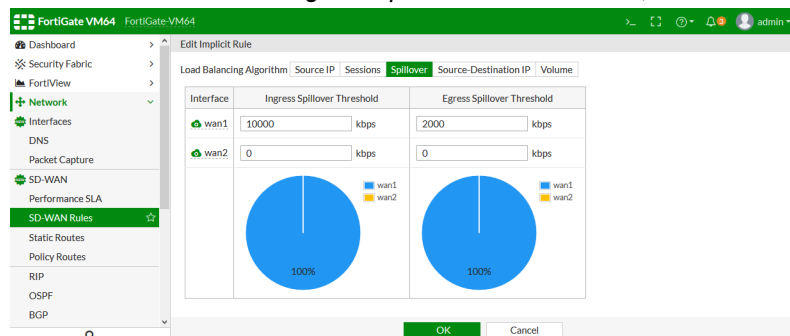
Example 4

Load balancing can be used to reduce costs when internet connections are charged at different rates. For example, if wan2 charges based on volume usage and wan1 charges a fixed monthly fee, we can use wan1 at its maximum bandwidth, and use wan2 for overflow.

In this example, wan1's bandwidth is 10Mbps down and 2Mbps up. Traffic will use wan1 until it reaches its spillover limit, then it will start to use wan2. Note that `auto-asic-offload` must be disabled in the firewall policy.

Using the GUI:

1. On the FortiGate, enable SD-WAN and add wan1 and wan2 as SD-WAN members, then add a policy and static route. See [Configuring the SD-WAN interface on page 452](#) for details.
2. Go to *Network > SD-WAN Rules*.
3. Edit the *sd-wan* rule (the last default rule).
4. For the *Load Balancing Algorithm*, select *Spillover*.
5. Enter 10000 in the *wan1 Ingress Spillover Threshold* field, and 2000 in the *wan1 Egress Spillover Threshold* field.



6. Click **OK**.

Using the CLI:

```
config system virtual-wan-link
    set load-balance-mode usage-based
    config members
        edit 1
            set interface "wan1"
            set spillover-threshold 2000
            set ingress-spillover-threshold 10000
        next
    end
end
```

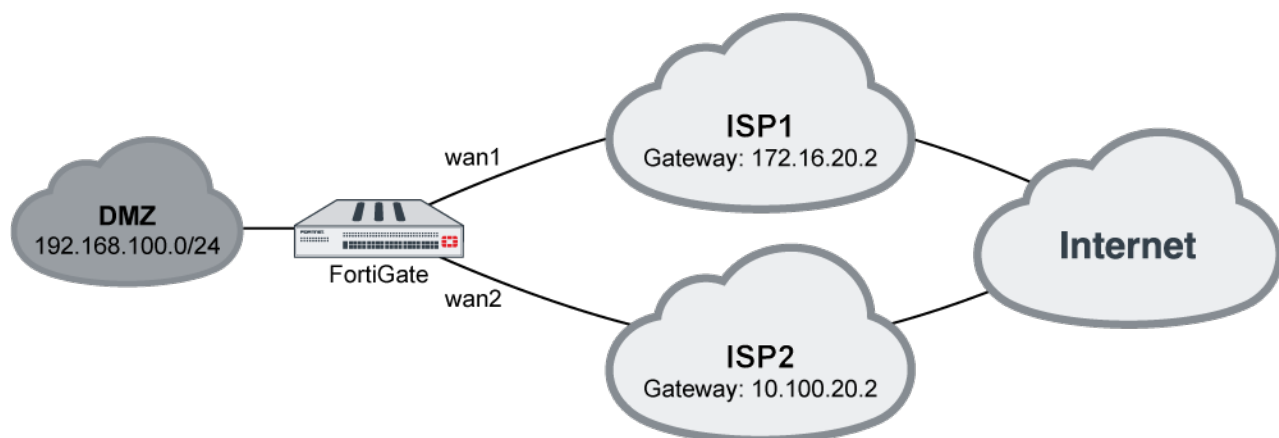
SD-WAN rules - best quality

SD-WAN rules are used to control how sessions are distributed to SD-WAN members. Rules can be configured in one of five modes:

- **auto**: Interfaces are assigned a priority based on quality.
- **Manual (manual)**: Interfaces are manually assigned a priority.
- **Best Quality (priority)**: Interface are assigned a priority based on the link-cost-factor of the interface.
- **Lowest Cost (SLA) (sla)**: Interfaces are assigned a priority based on selected SLA settings. See [SD-WAN rules - lowest cost \(SLA\) on page 475](#).
- **Maximize Bandwidth (SLA) (load-balance)**: Traffic is distributed among all available links based on the selected load balancing algorithm. See [SD-WAN rules - maximize bandwidth \(SLA\) on page 477](#).

When using *Best Quality* mode, SD-WAN will choose the best link to forward traffic by comparing the *link-cost-factor*, selected from one of the following:

GUI	CLI	Description
Latency	<code>latency</code>	Select a link based on latency.
Jitter	<code>jitter</code>	Select a link based on jitter.
Packet Loss	<code>packet-loss</code>	Select a link based on packet loss.
Downstream	<code>inbandwidth</code>	Select a link based on available bandwidth of incoming traffic.
Upstream	<code>outbandwidth</code>	Select a link based on available bandwidth of outgoing traffic.
Bandwidth	<code>bibandwidth</code>	Select a link based on available bandwidth of bidirectional traffic.
custom-profile-1	<code>custom-profile-1</code>	Select link based on customized profile. If selected, set the following weights: <ul style="list-style-type: none"> • <code>packet-loss-weight</code>: Coefficient of packet-loss. • <code>latency-weight</code>: Coefficient of latency. • <code>jitter-weight</code>: Coefficient of jitter. • <code>bandwidth-weight</code>: Coefficient of reciprocal of available bidirectional bandwidth.

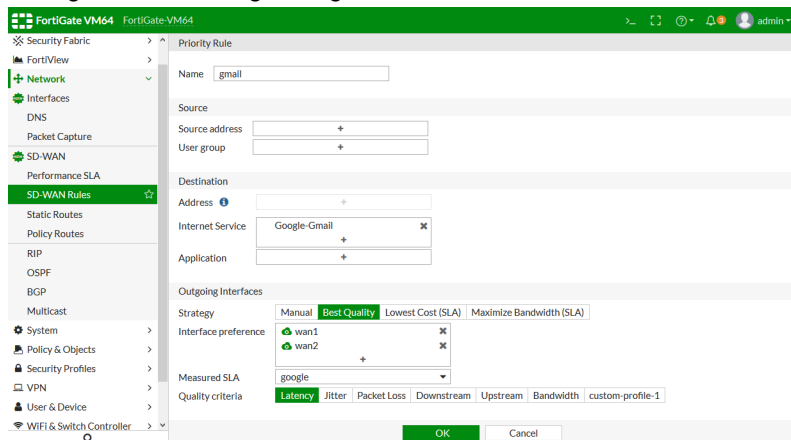


In this example, your wan1 and wan2 SD-WAN interfaces connect to two ISPs that both go to the public internet, and you want Gmail services to use the link with the least latency.

To configure an SD-WAN rule to use Best Quality:

1. On the FortiGate, enable SD-WAN and add wan1 and wan2 as SD-WAN members, then add a policy and static route. See [Configuring the SD-WAN interface on page 452](#) for details.
2. Create a new Performance SLA named *google*. See [Performance SLA - link monitoring on page 463](#).
3. Go to *Network > SD-WAN Rules*.
4. Click *Create New*. The *Priority Rule* page opens.
5. Enter a name for the rule, such as *gmail*.

6. Configure the following settings:



Field	Setting
Internet Service	Google-Gmail
Strategy	Best Quality
Interface preference	wan1 and wan2
Measured SLA	google (created in step 2).
Quality criteria	Latency

7. Click OK to create the rule.

To configure an SD-WAN rule to use priority:

```

config system virtual-wan-link
    config health-check
        edit "google"
            set server "google.com"
            set members 1 2
        next
    end
    config service
        edit 1
            set name "gmail"
            set mode priority
            set internet-service enable
            set internet-service-id 65646
            set health-check "google"
            set link-cost-factor latency
            set priority-members 1 2
        next
    end
end

```

To diagnose the Performance SLA status:

```

FGT # diagnose sys virtual-wan-link health-check google
Health Check(google):

```



```
Seq(1): state(alive), packet-loss(0.000%) latency(14.563), jitter(4.334) sla_map=0x0
Seq(2): state(alive), packet-loss(0.000%) latency(12.633), jitter(6.265) sla_map=0x0
```

```
FGT # diagnose sys virtual-wan-link service 1
```

```
Service(1):
```

```
TOS(0x0/0x0), protocol(0: 1->65535), Mode(priority), link-cost-factor(latency), link-
cost-threshold(10), health-check(google) Members:
```

```
1: Seq_num(2), alive, latency: 12.633, selected
2: Seq_num(1), alive, latency: 14.563, selected
```

```
Internet Service: Google-Gmail(65646)
```

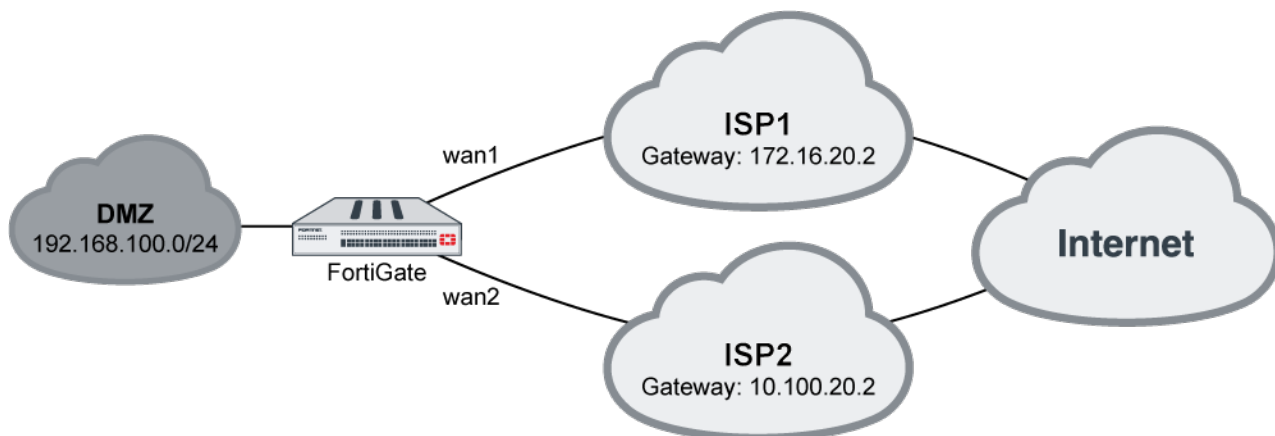
As wan2 has a smaller latency, SD-WAN will put Seq_num(2) on top of Seq_num(1) and wan2 will be used to forward Gmail traffic.

SD-WAN rules - lowest cost (SLA)

SD-WAN rules are used to control how sessions are distributed to SD-WAN members. Rules can be configured in one of five modes:

- **auto**: Interfaces are assigned a priority based on quality.
- **Manual (manual)**: Interfaces are manually assigned a priority.
- **Best Quality (priority)**: Interface are assigned a priority based on the link-cost-factor of the interface. See [SD-WAN rules - best quality on page 472](#).
- **Lowest Cost (SLA) (sla)**: Interfaces are assigned a priority based on selected SLA settings.
- **Maximize Bandwidth (SLA) (load-balance)**: Traffic is distributed among all available links based on the selected load balancing algorithm. See [SD-WAN rules - maximize bandwidth \(SLA\) on page 477](#).

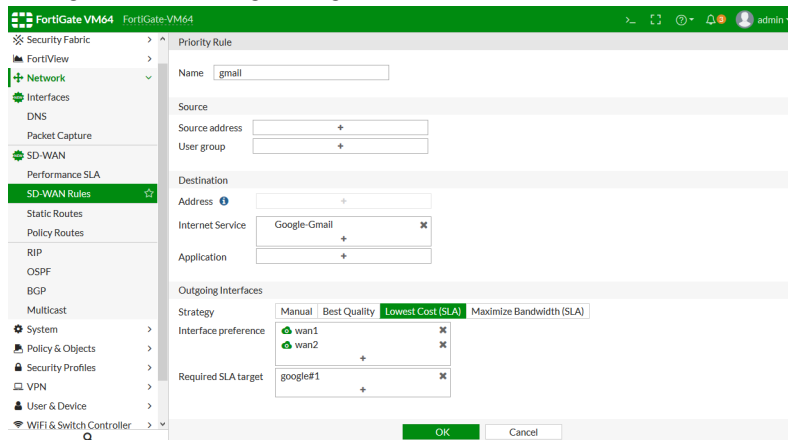
When using *Lowest Cost (SLA)* mode (`sla` in the CLI), SD-WAN will choose the lowest cost link that satisfies SLA to forward traffic. The lowest possible cost is 0. If multiple eligible links have the same cost, the *Interface preference* order will be used to select a link.



In this example, your wan1 and wan2 SD-WAN interfaces connect to two ISPs that both go to the public internet. The cost of wan2 is less than that of wan1. You want to configure Gmail services to use the lowest cost interface, but the link quality must meet a standard of latency: 10ms, and jitter: 5ms.

To configure an SD-WAN rule to use Lowest Cost (SLA):

1. On the FortiGate, enable SD-WAN and add wan1 and wan2 as SD-WAN members, then add a policy and static route. See [Configuring the SD-WAN interface on page 452](#) for details.
2. Create a new Performance SLA named *google* that includes an SLA Target 1 with *Latency threshold* = 10ms and *Jitter threshold* = 5ms. See [Performance SLA - link monitoring on page 463](#).
3. Go to *Network > SD-WAN Rules*.
4. Click *Create New*. The *Priority Rule* page opens.
5. Enter a name for the rule, such as *gmail*.
6. Configure the following settings:



Field	Setting
Internet Service	Google-Gmail
Strategy	Lowest Cost (SLA)
Interface preference	wan1 and wan2
Required SLA target	google#1 (created in step 2).

7. Click *OK* to create the rule.

To configure an SD-WAN rule to use sla:

```
config system virtual-wan-link
  config members
    edit 1
      set interface "wan1"
      set cost 10
    next
    edit 2
      set interface "wan2"
      set cost 5
    next
  end

  config health-check
    edit "google"
      set server "google.com"
```

```

        set members 1 2
    config sla
        edit 1
            set latency-threshold 10
            set jitter-threshold 5
        next
    end
next
end
config service
    edit 1
        set name "gmail"
        set mode sla
        set internet-service enable
        set internet-service-id 65646
        config sla
            edit "google"
                set id 1
            next
        end
        set priority-members 1 2
    next
end
end

```

To diagnose the Performance SLA status:

FGT # **diagnose sys virtual-wan-link health-check google**

Health Check(google):

Seq(1): state(alive), packet-loss(0.000%) latency(14.563), jitter(4.334) sla_map=0x0

Seq(2): state(alive), packet-loss(0.000%) latency(12.633), jitter(6.265) sla_map=0x0

FGT # **diagnose sys virtual-wan-link service 1**

Service(1): Address Mode(IPV4) flags=0x0

TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla)

Members:<
>

1: Seq_num(2), alive, sla(0x1), cfg_order(1), selected

2: Seq_num(1), alive, sla(0x1), cfg_order(0), selected

Internet Service: Google.Gmail(65646)

When both wan1 and wan2 meet the SLA requirements, Gmail traffic will only use wan2. If only wan1 meets the SLA requirements, Gmail traffic will only use wan1, even though it has a higher cost. If neither interface meets the requirements, wan2 will be used.

If both interface had the same cost and both met the SLA requirements, the first link configured in `set priority-members` would be used.

SD-WAN rules - maximize bandwidth (SLA)

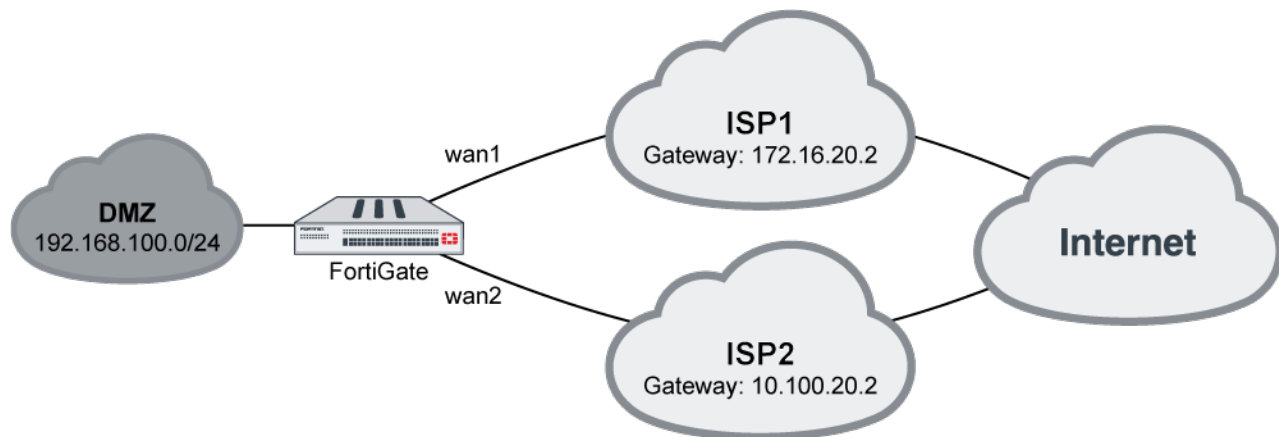
SD-WAN rules are used to control how sessions are distributed to SD-WAN members. Rules can be configured in one of five modes:

- **auto**: Interfaces are assigned a priority based on quality.
- **Manual (manual)**: Interfaces are manually assigned a priority.
- **Best Quality (priority)**: Interface are assigned a priority based on the link-cost-factor of the interface. See [SD-WAN rules - best quality on page 472](#).
- **Lowest Cost (SLA) (sla)**: Interfaces are assigned a priority based on selected SLA settings. See [SD-WAN rules - lowest cost \(SLA\) on page 475](#).
- **Maximize Bandwidth (SLA) (load-balance)**: Traffic is distributed among all available links based on the selected load balancing algorithm.

When using *Maximize Bandwidth* mode (`load-balance` in the CLI), SD-WAN will all of the links that satisfies SLA to forward traffic based on a round-robin load balancing algorithm.



ADVPN is not supported in this mode.

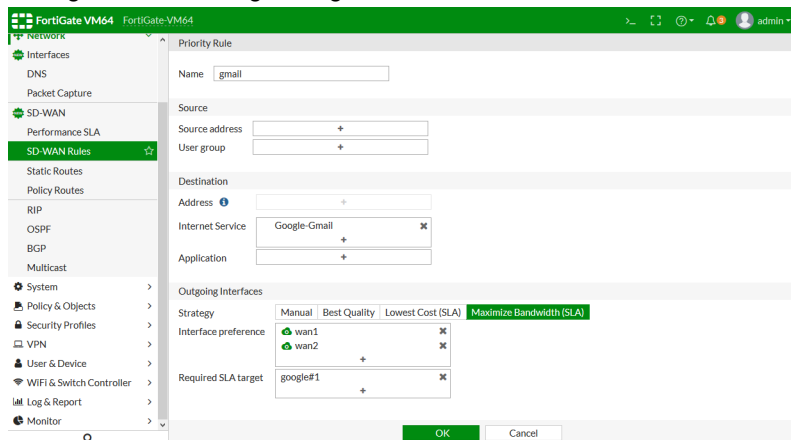


In this example, your wan1 and wan2 SD-WAN interfaces connect to two ISPs that both go to the public internet. You want to configure Gmail services to use both of the interface, but the link quality must meet a standard of latency: 10ms, and jitter: 5ms. This can maximize the bandwidth usage.

To configure an SD-WAN rule to use Maximize Bandwidth (SLA):

1. On the FortiGate, enable SD-WAN and add wan1 and wan2 as SD-WAN members, then add a policy and static route. See [Configuring the SD-WAN interface on page 452](#) for details.
2. Create a new Performance SLA named *google* that includes an SLA Target 1 with *Latency threshold* = 10ms and *Jitter threshold* = 5ms. See [Performance SLA - link monitoring on page 463](#).
3. Go to *Network > SD-WAN Rules*.
4. Click *Create New*. The *Priority Rule* page opens.
5. Enter a name for the rule, such as *gmail*.

6. Configure the following settings:



Field	Setting
Internet Service	Google-Gmail
Strategy	Maximize Bandwidth (SLA)
Interface preference	wan1 and wan2
Required SLA target	google#1 (created in step 2).

7. Click OK to create the rule.

To configure an SD-WAN rule to use SLA:

```

config system virtual-wan-link
    config health-check
        edit "google"
            set server "google.com"
            set members 1 2
            config sla
                edit 1
                    set latency-threshold 10
                    set jitter-threshold 5
                next
            end
        next
    end
end
config service
    edit 1
        set name "gmail"
        set mode load-balance
        set internet-service enable
        set internet-service-id 65646
        config sla
            edit "google"
                set id 1
            next
        end
        set priority-members 1 2
    next
end

```

```
end
end
```

To diagnose the performance SLA status:

```
FGT # diagnose sys virtual-wan-link health-check google
Health Check(google):
Seq(1): state(alive), packet-loss(0.000%) latency(14.563), jitter(4.334) sla_map=0x0
Seq(2): state(alive), packet-loss(0.000%) latency(12.633), jitter(6.265) sla_map=0x0

FGT # diagnose sys virtual-wan-link service 1
Service(1): Address Mode(IPV4) flags=0x0

TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance)
Members:<<BR>>

1: Seq_num(1), alive, sla(0x1), num of pass(1), selected
2: Seq_num(2), alive, sla(0x1), num of pass(1), selected

Internet Service: Google.Gmail(65646)
```

When both wan1 and wan2 meet the SLA requirements, Gmail traffic will use both wan1 and wan2. If only one of the interfaces meets the SLA requirements, Gmail traffic will only use that interface.

If neither interface meets the requirements but health-check is still alive, then wan1 and wan2 tie. The traffic will try to balance between wan1 and wan2, using both interfaces to forward traffic.

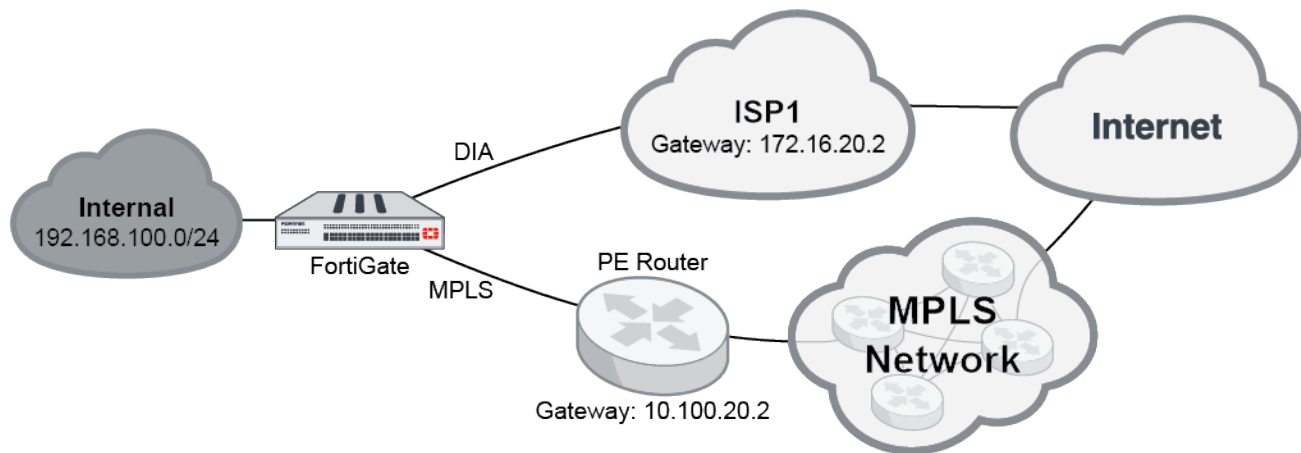
Application steering using SD-WAN rules

This topic covers how to use application steering in a topology with multiple WAN links. The following examples illustrate how to use different strategies to perform application steering to accommodate different business needs:

- [Static application steering with a manual strategy on page 480](#)
- [Dynamic application steering with lowest cost and best quality strategies on page 483](#)

Static application steering with a manual strategy

This example covers a typical usage scenario where the SD-WAN has two members: MPLS and DIA. DIA is primarily used for direct internet access to internet applications, such as Office365, Google applications, Amazon, and Dropbox. MPLS is primarily used for SIP, and works as a backup when DIA is not working.



This example configures all SIP traffic to use MPLS while all other traffic uses DIA. If DIA is not working, the traffic will use MPLS.

To configure an SD-WAN rule to use SIP and DIA in the GUI:

1. Add port1 (DIA) and port2 (MPLS) as SD-WAN members, and configure a static route. See [Configuring the SD-WAN interface on page 452](#) for details.
2. Create a firewall policy with an *Application Control* profile configured. See [Configuring security policies for SD-WAN on page 455](#) for details.
3. Go to *Network > SD-WAN Rules*.
4. Click *Create New*. The *Priority Rule* page opens.
5. Enter a name for the rule, such as *SIP*.
6. Click the *Application* field and select the applicable SIP applications from the *Select Entries* panel.
7. Under *Outgoing Interfaces*, set the *Strategy* to *Manual*.
8. For *Interface preference*, select *MPLS*.
9. Click *OK*.
10. Click *Create New* to create another rule.
11. Enter a name for the rule, such as *Internet*.
12. Click the *Address* field and select *all* from the panel.
13. Under *Outgoing Interfaces*, set the *Strategy* to *Manual*.

14. For *Interface preference*, select *DIA*.

15. Click **OK**.

To configure the firewall policy using the CLI:

```
config firewall policy
  edit 1
    set name "1"
    set srcintf "dmz"
    set dstintf "virtual-wan-link"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set fsso disable
    set application-list "default"
    set ssl-ssh-profile "certificate-inspection"
    set nat enable
  next
end
```

To configure an SD-WAN rule to use SIP and DIA using the CLI:

```
config system virtual-wan-link
  set status enable
  config members
    edit 1
      set interface "MPLS"
    next
    edit 2
      set interface "DIA"
    next
  end
  config service
    edit 1
      set name "SIP"
```



```

        set internet-service enable
        set internet-service-app-ctrl 34640 152305677 38938 26180 26179 30251
        set priority-members 1
    next
    edit 2
        set name "Internet"
        set input-device "dmz"
        set dst "all"
        set priority-members 2
    next
end
end

```

All SIP traffic uses MPLS. All other traffic goes to DIA. If DIA is broken, the traffic uses MPLS. If you use VPN instead of MPLS to run SIP traffic, you must configure a VPN interface, for example vpn1, and then replace member 1 from MPLS to vpn1 for SD-WAN member.

To use the diagnose command to check performance SLA status using the CLI:

```

# diagnose sys virtual-wan-link service 1

Service(1): Address Mode(IPV4) flags=0x0

TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Members:<<BR>>

1: Seq_num(1), alive, selected

Internet Service: SIP(4294836224 34640) SIP.Method(4294836225 152305677) SIP.Via.NAT
(4294836226 38938) SIP_Media.Type.Application(4294836227 26180) SIP_Message(4294836228
26179) SIP_Voice(4294836229 30251)

# diagnose sys virtual-wan-link service 2

Service(2): Address Mode(IPV4) flags=0x0

TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Members:<<BR>>

1: Seq_num(2), alive, selected

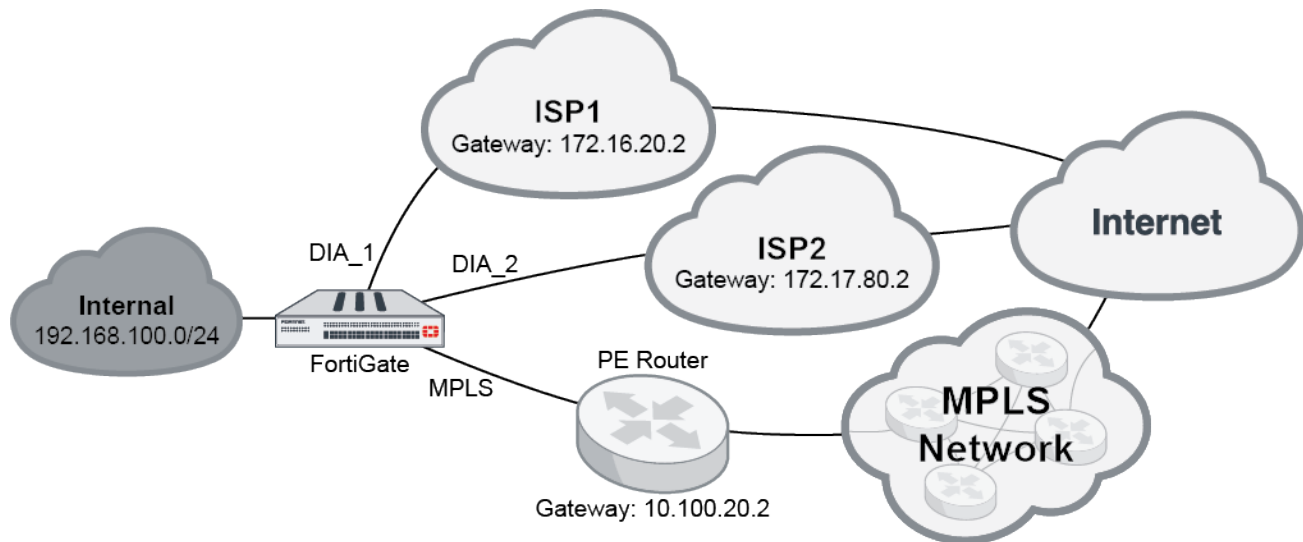
Dst address: 0.0.0.0-255.255.255.255

# diagnose sys virtual-wan-link internet-service-app-ctrl-list
Ctrl application(SIP 34640):Internet Service ID(4294836224)
Ctrl application(SIP.Method 152305677):Internet Service ID(4294836225)
Ctrl application(SIP.Via.NAT 38938):Internet Service ID(4294836226)
Ctrl application(SIP_Media.Type.Application 26180):Internet Service ID(4294836227)
Ctrl application(SIP_Message 26179):Internet Service ID(4294836228)
Ctrl application(SIP_Voice 30251):Internet Service ID(4294836229)

```

Dynamic application steering with lowest cost and best quality strategies

In this example, the SD-WAN has three members: two ISPs (DIA_1 and DIA_2) that are used for access to internet applications, and an MPLS link that is used exclusively as a backup for business critical applications.



Business applications, such as Office365, Google, Dropbox, and SIP, use the *Lowest Cost (SLA)* strategy to provide application steering, and traffic falls back to MPLS only if both ISP1 and ISP2 are down. Non-business applications, such as Facebook and Youtube, use the *Best Quality* strategy to choose between the ISPs.

To configure the SD-WAN members, static route, and firewall policy in the GUI:

1. Add port1 (DIA_1), port2 (DIA_2), and port3 (MPLS) as SD-WAN members. Set the cost of DIA_1 and DIA_2 to 0, and MPLS to 20. See [Configuring the SD-WAN interface on page 452](#) for details.

New SD-WAN Member x

Interface	MPLS (port3)
Gateway	10.100.20.2
Cost	20
Status	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable

2. Configure a static route. See [Adding a static route on page 454](#) for details.
3. Create a firewall policy to allow traffic out on SD-WAN, with an *Application Control* profile configured. See [Configuring security policies for SD-WAN on page 455](#) for details.

To configure the SD-WAN rule and performance SLA checks for business critical application in the GUI:

1. Go to *Network > SD-WAN Rules*, and click *Create New*.
2. Set the name to *BusinessCriticalApps*.
This rule will steer your business critical traffic to the appropriate link based on the *Lowest Cost (SLA)*.
3. Set *Source address* to *all*.
4. Under *Destination*, set *Application* to your required applications. In this example: *Microsoft.Office.365*, *Microsoft.Office.Online*, *Google.Docs*, *Dropbox*, and *SIP*.
5. Under *Outgoing Interfaces*, set *Strategy* to *Lowest Cost (SLA)*.
The lowest cost is defined in the SD-WAN member interface settings (see [Configuring the SD-WAN interface on page 452](#)). The lowest possible cost is 0, which represents the most preferred link. In this example, DIA_1 and DIA_2 both have a cost of 0, while MPLS has a cost of 20 because it is used for backup.
6. In *Interface preference*, add the interfaces in order of preference when the cost of the links is tied. In this example, DIA_1, DIA_2, then MPLS.

MPLS will always be chosen last, because it has the highest cost. DIA_1 and DIA_2 have the same cost, so an interface is selected based on their order in the *Interface preference* list.

7. Set *Required SLA target* to ensure that only links that pass your SLA target are chosen in this SD-WAN rule:

- a. Click in the *Required SLA target* field.
- b. In the *Select Entries* pane, click *Create*. The *New Performance SLA* pane opens.
- c. Set *Name* to *BusinessCritical_HC*.
This health check is used for business critical applications in your SD-WAN rule.
- d. Leave *Protocol* set to *Ping*, and add up to two servers, such as *office.com* and *google.com*.
- e. Set *Participants* to all three interfaces: DIA_1, DIA_2, and MPLS.
- f. Under *SLA Target* click *Add Target*.

The attributes in your target determine the quality of your link. The SLA target of each link is compared when determining which link to use based on the lowest cost. Links that meet the SLA target are preferred over links that fail, and move to the next step of selection based on cost. If no links meet the SLA target, then they all move to the next step.

In this example, disable *Latency threshold* and *Jitter threshold*, and set *Packet loss threshold* to 1.

- g. Click *OK*.
- h. Select the new performance SLA to set it as the *Required SLA target*.

When multiple SLA targets are added, you can choose which target to use in the SD-WAN rule.

8. Click *OK* to create the SD-WAN rule.

To configure the SD-WAN rule and performance SLA checks for non-business critical application in the GUI:

1. Go to *Network > SD-WAN Rules*, and click *Create New*.
2. Set the name to *NonBusinessCriticalApps*.
This rule will steer your non-business critical traffic to the appropriate link based on the *Best Quality*. No SLA target must be met, as the best link is selected based on the configured quality criteria and interface preference order.
3. Set *Source address* to *all*.

4. Under *Destination*, set *Application* to your required applications. In this example: *Facebook*, and *Youtube*.
5. Under *Outgoing Interfaces*, set *Strategy* to *Best Quality*.
6. In *Interface preference*, add the interfaces in order of preference.
By default, a more preferred link has an advantage of 10% over a less preferred link. For example, when latency is used, the preferred link's calculated latency = real latency / (1+10%).

The preferred link advantage can be customized in the CLI when the mode is `priority` (*Best Quality*) or `auto`:



```
config system virtual-wan-link
  config service
    edit <id>
      set link-cost-threshold <integer>
    next
  end
end
```

7. Create and apply a new performance SLA profile:
 - a. Click in the *Measured SLA* field.
 - b. In the drop-down list, click *Create*. The *New Performance SLA* pane opens.
 - c. Set *Name* to *NonBusinessCritical_HC*.
This health check is used for non-business critical applications in your SD-WAN rule.
 - d. Leave *Protocol* set to *Ping*, and add up to two servers, such as *youtube.com* and *facebook.com*.
 - e. Set *Participants* to the *DIA_1* and *DIA_2* interfaces. In this example, MPLS is not used for non-business critical applications.
 - f. Leave *SLA Target* disabled.
 - g. Click *OK*.
 - h. Select the new performance SLA from the list to set it as the *Measured SLA*.
8. Set *Quality criteria* as required. In this example, *Latency* is selected.
For bandwidth related criteria, such as *Downstream*, *Upstream*, and *Bandwidth* (bi-directional), the selection is based on available bandwidth. An estimated bandwidth should be configured on the interface to provide a baseline, maximum available bandwidth.

Priority Rule

Name:

Source

Source address: + ✕

User group: +

Destination

Address: +

Internet Service: +

Application: ✕
 ✕
+

Outgoing Interfaces

Strategy: + ✕
☒ Best Quality
☐ Lowest Cost (SLA)
☐ Maximize Bandwidth (SLA)

Interface preference: ☒ DIA_1 (port1) ✕
☒ DIA_2 (port2) ✕
+

Measured SLA: + ✕

Quality criteria: + ✕

Status: ☒ Enable ☐ Disable

OK Cancel

9. Click OK to create the SD-WAN rule.

To configure the SD-WAN members, static route, and firewall policy in the CLI:

1. Configure the interfaces:

```
config system interface
  edit "port1"
    set ip <class_ip&net_netmask>
    set alias "DIA_1"
    set role wan
  next
  edit "port2"
    set ip <class_ip&net_netmask>
    set alias "DIA_2"
    set role wan
  next
  edit "port3"
    set ip <class_ip&net_netmask>
    set alias "MPLS"
    set role wan
  next
end
```

2. Configure the SD-WAN members:

```
config system virtual-wan-link
  set status enable
  config members
    edit 1
      set interface "port1"
      set gateway 172.16.20.2
    next
    edit 2
      set interface "port2"
      set gateway 172.17.80.2
```

```
        next
    edit 3
        set interface "port3"
        set gateway 10.100.20.2
        set cost 20
    next
end
end
```

To configure the SD-WAN rule and performance SLA checks for business critical application in the CLI:

1. Configure the *BusinessCriticalApps_HC* health-check:

```
config system virtual-wan-link
    config health-check
        edit "BusinessCriticalApps_HC"
            set server "office.com" "google.com"
            set members 1 2 3
            config sla
                edit 1
                    set link-cost-factor packet-loss
                    set packetloss-threshold 1
                next
            end
        next
    end
end
```

2. Configure the *BusinessCriticalApps* service to use *Lowest Cost (SLA)*:

```
config system virtual-wan-link
    config service
        edit 1
            set name "BusinessCriticalApps"
            set mode sla
            set src "all"
            set internet-service enable
            set internet-service-app-ctrl 17459 16541 33182 16177 34640
            config sla
                edit "BusinessCriticalApps_HC"
                    set id 1
                next
            end
            set priority-members 1 2 3
        next
    end
end
```

To configure the SD-WAN rule and performance SLA checks for non-business critical application in the CLI:

1. Configure the *nonBusinessCriticalApps_HC* health-check:

```
config system virtual-wan-link
    config health-check
        edit "NonBusinessCriticalApps_HC"
            set server "youtube.com" "facebook.com"
```

```

        set members 1 2
    next
end
end

```

2. Configure the *BusinessCriticalApps* service to use *Lowest Cost (SLA)*:

```

config system virtual-wan-link
    config service
        edit 4
            set name "NonBusinessCriticalApps"
            set mode priority
            set src "all"
            set internet-service enable
            set internet-service-app-ctrl 15832 31077
            set health-check "NonBusinessCriticalApps_HC"
            set priority-members 1 2
        next
    end
end

```

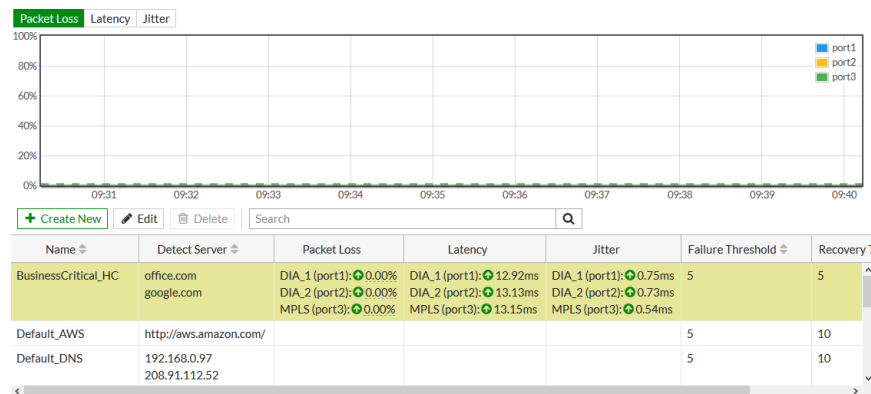
Verification

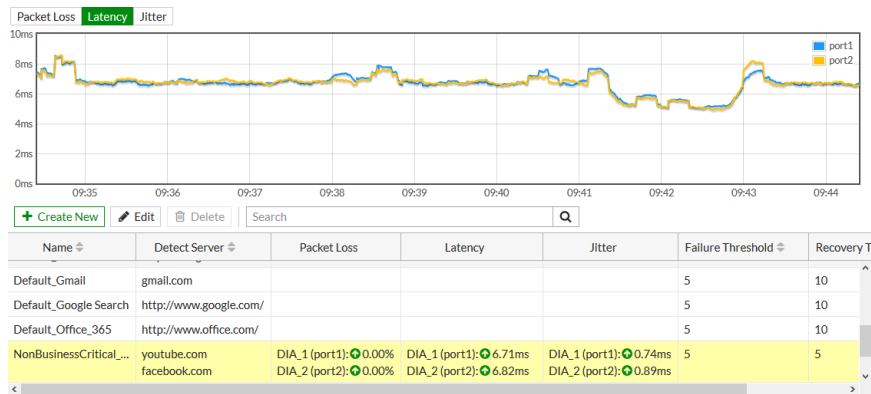
Check the following GUI pages, and run the following CLI commands to confirm that your traffic is being steered by the SD-WAN rules.

Health checks

To verify the status of each of the health checks in the GUI:

- Go to **Network > Performance SLA** and select each of the health checks from the list.














To verify the status of each of the health checks in the CLI:

```
# diagnose sys virtual-wan-link health-check
Health Check(BusinessCritical_HC):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(12.884), jitter(0.919) sla_map=0x1
Seq(2 port2): state(alive), packet-loss(0.000%) latency(13.018), jitter(0.723) sla_map=0x1
Seq(3 port3): state(alive), packet-loss(0.000%) latency(13.018), jitter(0.923) sla_map=0x1
Health Check(NonBusinessCritical_HC):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(6.888), jitter(0.953) sla_map=0x0
Seq(2 port2): state(alive), packet-loss(0.000%) latency(6.805), jitter(0.830) sla_map=0x0
```

Rule members and hit count

To verify the active members and hit count of the SD-WAN rule in the GUI:

1. Go to *Network > SD-WAN Rules*.

<div><div>+ Create New</div><div>Edit</div><div>Delete</div></div>		<div><div>Search</div><div>Q</div></div>			
ID	Name	Source	Destination	Criteria	Members
IPv4 2					
1	BusinessCriticalApps	 all	Dropbox Google.Docs Microsoft.Office.365 Microsoft.Office.Online SIP	SLA	 DIA_1 (port1)  DIA_2 (port2)  MPLS (port3)
4	NonBusinessCriticalApps	 all	Facebook YouTube	Latency	 DIA_1 (port1)  DIA_2 (port2)
Implicit 1					
	sd-wan	 all	 all	Sessions	<input type="checkbox"/> any

To verify the active members and hit count of the SD-WAN rule in the CLI:

```
# diagnose sys virtual-wan-link service

Service(3): Address Mode(IPV4) flags=0x0
Gen(13), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
Members:
  1: Seq_num(1 port1), alive, sla(0x1), cfg_order(0), cost(0), selected
  2: Seq_num(2 port2), alive, sla(0x1), cfg_order(1), cost(0), selected
  3: Seq_num(3 port3), alive, sla(0x1), cfg_order(2), cost(20), selected
Internet Service: Dropbox(4294836727,0,0,0 17459) Google.Docs(4294836992,0,0,0 16541)
Microsoft.Office.365(4294837472,0,0,0 33182) Microsoft.Office.Online(4294837475,0,0,0 16177)
SIP(4294837918,0,0,0 34640)
Src address:
  0.0.0.0-255.255.255.255
```

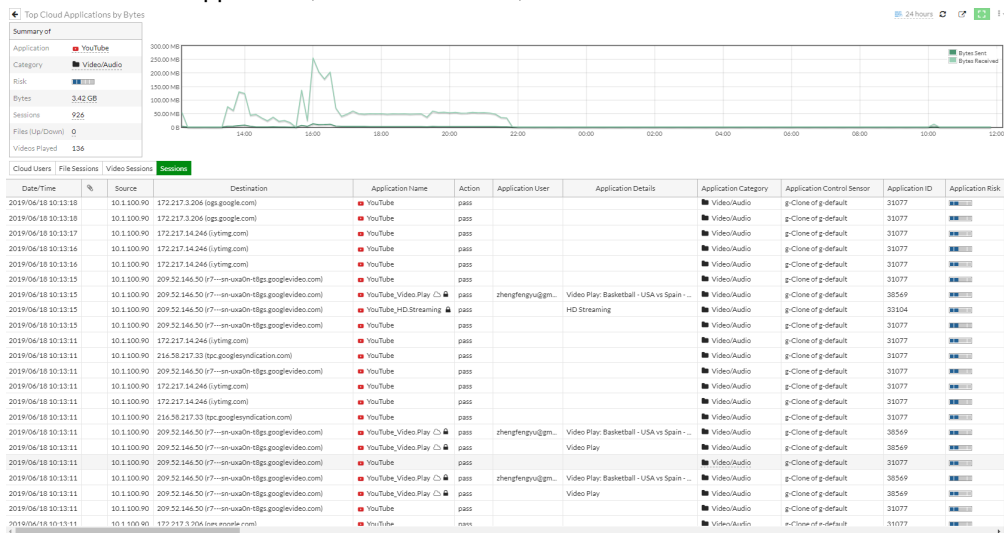


```
Service(4): Address Mode(IPV4) flags=0x0
  Gen(211), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(latency),
link-cost-threshold(10), heath-check(NonBusinessCritical_HC)
Members:
  1: Seq_num(1 port1), alive, latency: 5.712, selected
  2: Seq_num(2 port2), alive, latency: 5.511, selected
Internet Service: Facebook(4294836806,0,0,0 15832) YouTube(4294838537,0,0,0 31077)
Src address:
  0.0.0.0-255.255.255.255
```

Applications and sessions

To verify sessions in FortiView:

1. Go to a dashboard and add the *FortiView Top N* widget configured for cloud applications and sorted by bytes. See [Configuring the Cloud Applications widget on page 289](#) for details.
2. Drill down on an application, such as *YouTube*, then select the *Sessions* tab.



To verify applications identified by Application Control in SD-WAN:

```
# diagnose sys virtual-wan-link internet-service-app-ctrl-list
```

```
Facebook(15832 4294836697): 31.13.67.20 6 443 Fri April 17 22:33:39 2020
Facebook(15832 4294836697): 31.13.67.35 6 443 Fri April 17 22:33:41 2020
Facebook(15832 4294836697): 31.13.70.36 6 443 Fri April 17 22:36:41 2020
Facebook(15832 4294836697): 157.240.11.22 6 443 Fri April 17 22:36:42 2020
Facebook(15832 4294836697): 157.240.11.35 6 443 Fri April 17 22:36:41 2020
YouTube(31077 4294838227): 172.217.24.150 6 443 Fri April 17 22:32:16 2020
YouTube(31077 4294838227): 172.217.25.78 6 443 Fri April 17 22:32:16 2020
YouTube(31077 4294838227): 216.58.220.129 6 443 Fri April 17 22:32:34 2020
```

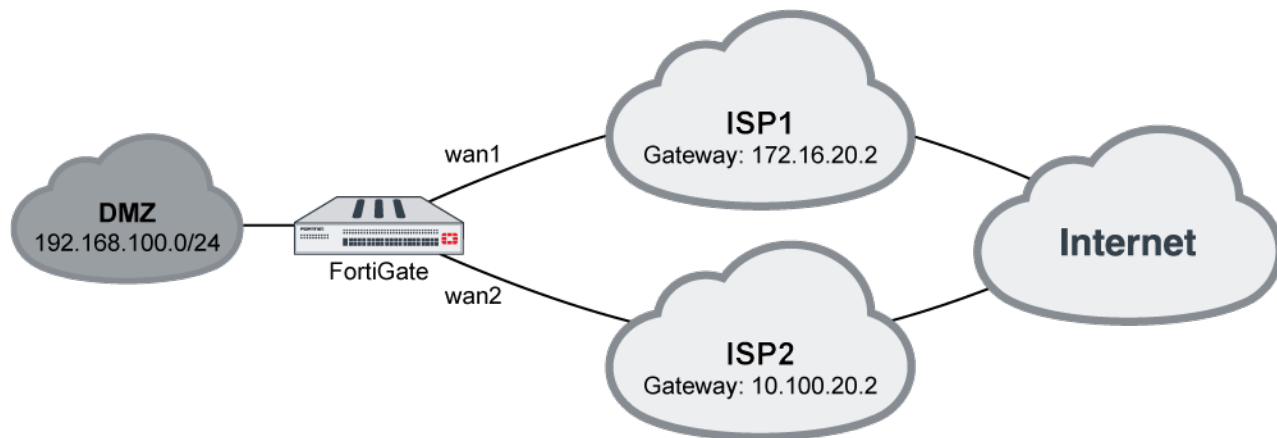
SD-WAN traffic shaping and QoS

Use a traffic shaper in a firewall shaping policy to control traffic flow. You can use it to control maximum and guaranteed bandwidth, or put certain traffic to one of the three different traffic priorities: high, medium, or low.

An advanced shaping policy can classify traffic into 30 groups. Use a shaping profile to define the percentage of the interface bandwidth that is allocated to each group. Each group of traffic is shaped to the assigned speed limit based on the outgoing bandwidth limit configured on the interface.

For more information, see the online help on shared policy traffic shaping and interface-based traffic shaping.

Sample topology



Sample configuration

This example shows a typical customer usage where the customer's SD-WAN has two member: wan1 and wan2 and each is 10Mb/s.

An overview of the procedures to configure SD-WAN traffic shaping and QoS with SD-WAN includes:

1. Give HTTP/HTTPS traffic high priority and give FTP low priority so that if there are conflicts, FortiGate will forward HTTP/HTTPS traffic first.
2. Even though FTP has low priority, configure FortiGate to give it a 1Mb/s guaranteed bandwidth on each SD-WAN member so that if there is no FTP traffic, other traffic can use all the bandwidth. If there is heavy FTP traffic, it can still be guaranteed a 1Mb/s bandwidth.
3. Traffic going to specific destinations such as a VOIP server uses wan1 to forward, and SD-WAN forwards with an Expedited Forwarding (EF) DSCP tag 101110.

To configure SD-WAN traffic shaping and QoS with SD-WAN in the GUI:

1. On the FortiGate, enable SD-WAN and add wan1 and wan2 as SD-WAN members, then add a policy and static route.
See [Configuring the SD-WAN interface on page 452](#).
2. When you add a firewall policy, enable *Application Control*.
3. Go to *Policy & Objects > Traffic Shapers* and edit *low-priority*.
 - a. Enable *Guaranteed Bandwidth* and set it to 1000 kbps.

4. Go to *Policy & Objects > Traffic Shaping Policy* and click *Create New*.
 - a. Name the traffic shaping policy, for example, *HTTP-HTTPS*.
 - b. Click the *Source* box and select *all*.
 - c. Click the *Destination* box and select *all*.
 - d. Click the *Service* box and select *HTTP* and *HTTPS*.
 - e. Click the *Outgoing Interface* box and select *SD-WAN*.
 - f. Enable both *Shared Shaper* and *Reverse Shaper* and select *high-priority* for both options.
 - g. Click *OK*.
5. Go to *Policy & Objects > Traffic Shaping Policy* and click *Create New*.
 - a. Name the traffic shaping policy, for example, *FTP*.
 - b. Click the *Source* box and select *all*.
 - c. Click the *Destination* box and select *all*.
 - d. Click the *Service* box and select *FTP*, *FTP_GET*, and *FTP_PUT*.
 - e. Click the *Outgoing Interface* box and select *SD-WAN*.
 - f. Enable both *Shared Shaper* and *Reverse Shaper* and select *low-priority* for both options.
 - g. Click *OK*.
6. Go to *Network > SD-WAN Rules* and click *Create New*.
 - a. Enter a name for the rule, such as *Internet*.
 - b. In the *Destination* section, click the *Address* box and select the VOIP server you created in the firewall address.
 - c. For *Strategy*, select *Manual*.
 - d. For *Interface preference*, select *wan1*.
 - e. Click *OK*.
7. Use CLI commands to modify DSCP settings. See the DSCP CLI commands below.

To configure the firewall policy using the CLI:

```
config firewall policy
  edit 1
    set name "1"
    set srcintf "dmz"
    set dstintf ""virtual-wan-link""
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set nat enable
  next
end
```

To configure the firewall traffic shaper priority using the CLI:

```
config firewall shaper traffic-shaper
  edit "high-priority"
    set maximum-bandwidth 1048576
    set per-policy enable
  next
  edit "low-priority"
    set guaranteed-bandwidth 1000
    set maximum-bandwidth 1048576
```

```
        set priority low
        set per-policy enable
    next
end
```

To configure the firewall traffic shaping policy using the CLI:

```
config firewall shaping-policy
    edit 1
        set name "http-https"
        set service "HTTP" "HTTPS"
        set dstintf "virtual-wan-link"
        set traffic-shaper "high-priority"
        set traffic-shaper-reverse "high-priority"
        set srcaddr "all"
        set dstaddr "all"
    next
    edit 2
        set name "FTP"
        set service "FTP" "FTP_GET" "FTP_PUT"
        set dstintf "virtual-wan-link"
        set traffic-shaper "low-priority"
        set traffic-shaper-reverse "low-priority"
        set srcaddr "all"
        set dstaddr "all"
    next
end
```

To configure SD-WAN traffic shaping and QoS with SD-WAN in the CLI:

```
config system virtual-wan-link
    set status enable
    config members
        edit 1
            set interface "wan1"
            set gateway x.x.x.x
        next
        edit 2
            set interface "wan2"
            set gateway x.x.x.x
        next
    end
    config service
        edit 1
            set name "SIP"
            set dst "voip-server"
            set dscp-forward enable
            set dscp-forward-tag 101110
            set priority-members 1
        next
    end
end
```

To use the diagnose command to check if specific traffic is attached to the correct traffic shaper:

```
# diagnose firewall iprope list 100015

policy index=1 uuid_idx=0 action=accept
flag (0):
shapers: orig=high-priority(2/0/134217728) reply=high-priority(2/0/134217728)
cos_fwd=0 cos_rev=0
group=00100015 av=00000000 au=00000000 split=00000000
host=0 chk_client_info=0x0 app_list=0 ips_view=0
misc=0 dd_type=0 dd_mode=0
zone(1): 0 -> zone(2): 36 38
source(1): 0.0.0.0-255.255.255.255, uuid_idx=6,
dest(1): 0.0.0.0-255.255.255.255, uuid_idx=6,
service(2):
    [6:0x0:0/(1,65535)->(80,80)] helper:auto
    [6:0x0:0/(1,65535)->(443,443)] helper:auto

policy index=2 uuid_idx=0 action=accept
flag (0):
shapers: orig=low-priority(4/128000/134217728) reply=low-priority(4/128000/134217728)
cos_fwd=0 cos_rev=0
group=00100015 av=00000000 au=00000000 split=00000000
host=0 chk_client_info=0x0 app_list=0 ips_view=0
misc=0 dd_type=0 dd_mode=0
zone(1): 0 -> zone(2): 36 38
source(1): 0.0.0.0-255.255.255.255, uuid_idx=6,
dest(1): 0.0.0.0-255.255.255.255, uuid_idx=6,
service(3):
    [6:0x0:0/(1,65535)->(21,21)] helper:auto
    [6:0x0:0/(1,65535)->(21,21)] helper:auto
    [6:0x0:0/(1,65535)->(21,21)] helper:auto

FGT_A (root) #
```

To use the diagnose command to check if the correct traffic shaper is applied to the session:

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=11 expire=3599 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=5
origin-shaper=low-priority prio=4 guarantee 128000Bps max 1280000Bps traffic 1050Bps drops
0B
reply-shaper=
per_ip_shaper=
class_id=0 shaping_policy_id=2 ha_id=0 policy_dir=0 tunnel=/ helper=ftp vlan_cos=0/255
state=may_dirty npu npd os mif route_preserve
statistic(bytes/packets/allow_err): org=868/15/1 reply=752/10/1 tuples=2
tx speed(Bps/kbps): 76/0 rx speed(Bps/kbps): 66/0
orgin->sink: org pre->post, reply pre->post dev=39->38/38->39 gwy=172.16.200.55/0.0.0.0
hook=post dir=org act=snat 10.1.100.11:58241->172.16.200.55:21(172.16.200.1:58241)
hook=pre dir=reply act=dnat 172.16.200.55:21->172.16.200.1:58241(10.1.100.11:58241)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=4
serial=0003255f tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
```

```
npu_state=0x100000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0,
vlan=0x0000/0x0000
vlfid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:  offload-denied helper
total session 1
```

To use the diagnose command to check the status of a shared traffic shaper:

```
# diagnose firewall shaper traffic-shaper list

name high-priority
maximum-bandwidth 131072 KB/sec
guaranteed-bandwidth 0 KB/sec
current-bandwidth 0 B/sec
priority 2
tos ff
packets dropped 0
bytes dropped 0

name low-priority
maximum-bandwidth 131072 KB/sec
guaranteed-bandwidth 125 KB/sec
current-bandwidth 0 B/sec
priority 4
tos ff
packets dropped 0
bytes dropped 0

name high-priority
maximum-bandwidth 131072 KB/sec
guaranteed-bandwidth 0 KB/sec
current-bandwidth 0 B/sec
priority 2
policy 1
tos ff
packets dropped 0
bytes dropped 0

name low-priority
maximum-bandwidth 131072 KB/sec
guaranteed-bandwidth 125 KB/sec
current-bandwidth 0 B/sec
priority 4
policy 2
tos ff
packets dropped 0
bytes dropped 0
```

Per-link controls for policies and SLA checks

Firewall policies can use SD-WAN members as source and destination interfaces. This allows controlling traffic so that certain types of traffic can only use certain SD-WAN members.

Per link health-check parameters are supported in SLA configurations using the following CLI command:

```
config system virtual-wan-link
  config service
    edit <priority_rule>
      set sla-compare-method number
    next
  end
end
```

SLA values are compared based on the number of satisfied health checks, and health checks are limited to configured member interfaces only. The member with the most health check passes is set as the priority member. This only applies to SLA mode and load balance mode rules.

Example

In this example, a customer has four health checks and two SD-WAN members:

- health-check1 and health-check2 check SD-WAN member1
- health-check3 and health-check4 check SD-WAN member2

The customer wants traffic going to destination A to use the SD-WAN member that passes the most SLAs. For example, if health-check1 fails, then member1 only has one pass, while member2 has two passes, and traffic will use member2 for forwarding. If both checks fail for member2, then traffic would use member1.

To configure the FortiGate device:

```
config system virtual-wan-link
  config members
    edit 1
      set interface "port1"
    next
    edit 2
      set interface "port2"
    next
  end
  config health-check
    edit "ping1"
      set server "x.x.x.x"
      set members 1
      config sla
        edit 1
        next
      end
    next
    edit "ping2"
      set server "x.x.x.x"
      set members 1
      config sla
        edit 1
        next
      end
    next
    edit "ping3"
      set server "x.x.x.x"
      set members 2
      config sla
```

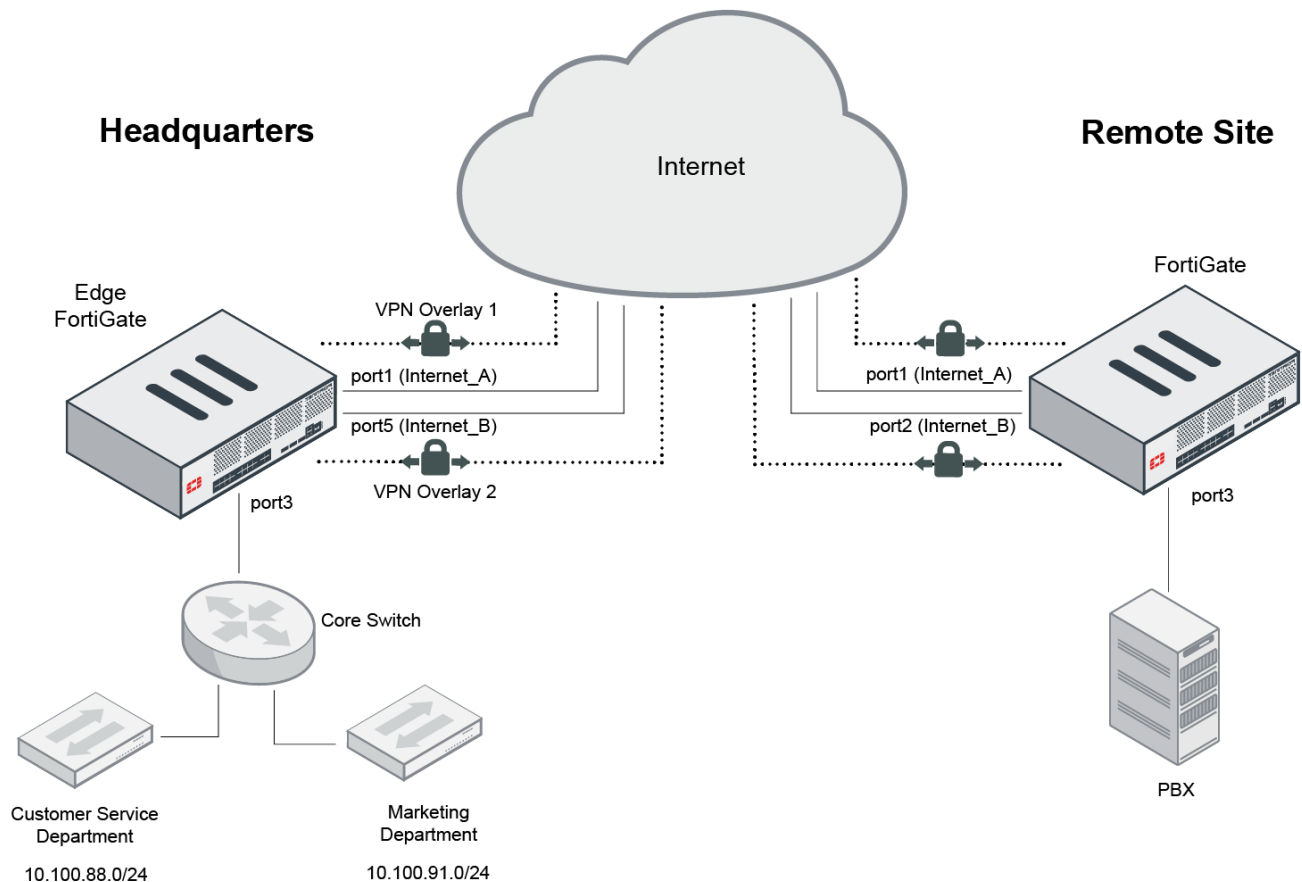
```
        edit 1
        next
    end
next
edit "ping4"
    set server "x.x.x.x"
    set members 2
    config sla
        edit 1
        next
    end
next
end
config service
    edit 1
        set mode sla
        set dst "destination-A"
        config sla
            edit "ping1"
                set id 1
            next
            edit "ping2"
                set id 1
            next
            edit "ping3"
                set id 1
            next
            edit "ping4"
                set id 1
            next
        end
        set priority-members 1 2
        set sla-compare-method number
    next
end
end
```

DSCP tag-based traffic steering in SD-WAN

This document demonstrates the Differentiated Services Code Point (DSCP) tag-based traffic steering in Fortinet secure SD-WAN. You can use this guide as an example to deploy DSCP tag-based traffic steering in Fortinet secure SD-WAN.

DSCP tags are often used to categorize traffic to provide quality of service (QoS). Based on DSCP tags, you can provide SD-WAN traffic steering on an edge device.

In this example, we have two different departments at the Headquarters site - Customer Service and Marketing. Traffic from each of these departments is marked with separate DSCP tags by the core switch, and passes through the core switch to the edge FortiGate. The edge FortiGate reads the DSCP tags and steers traffic to the preferred interface based on the defined SD-WAN rules.



In our example, we consider two types of traffic - social media traffic and VoIP traffic. VoIP traffic from Customer Service is considered to be more important than social media traffic. Each of these traffic types is marked with a DSCP tag by the core switch - VoIP traffic is marked with the DSCP tag of 011100, and social media traffic is marked with the DSCP tag of 001100. The DSCP tagged traffic is then passed on to the edge FortiGate. The edge FortiGate identifies the DSCP tagged traffic and based on the defined SD-WAN rules, the edge FortiGate steers:

- VoIP traffic to the preferred VPN overlay with the least jitter in order to provide the best quality of voice communication with the remote VoIP server (PBX)
- Social media traffic to the preferred Internet link with a lower cost (less expensive and less reliable)

If you are familiar with SD-WAN configurations in FortiOS, you can directly jump to the [Configuring SD-WAN rules on page 501](#) section to learn how to configure the SD-WAN rules to perform traffic steering. Otherwise, you can proceed with all of the following topics to configure the edge FortiGate:

- [Configuring IPsec tunnels on page 500](#)
- [Configuring SD-WAN interfaces on page 500](#)
- [Configuring firewall policies on page 501](#)
- [Configuring Performance SLA test on page 501](#)
- [Configuring SD-WAN rules on page 501](#)
- [Results on page 505](#)

Configuring IPsec tunnels

In our example, we have two interfaces `Internet_A (port1)` and `Internet_B (port5)` on which we have configured IPsec tunnels `Branch-HQ-A` and `Branch-HQ-B` respectively. To learn how to configure IPsec tunnels, refer to the [IPsec VPNs on page 1114](#) section.

After you have configured the IPsec tunnels as required, verify your IPsec tunnels by navigating to `VPN > IPsec Tunnels` in the GUI.

<div><div>+ Create New</div></div>		<div><div>Edit</div></div>	<div><div>Delete</div></div>	<div><div>Search</div></div>
	<div>Tunnel ▾</div>	<div>Interface Binding ▾</div>		
<div><div>☐</div> <div>☐ Custom 5</div></div>				
<div>⬇️</div>	<div>AWS_VPG</div>	<div>🏠</div>	<div>Internet_A (port1)</div>	
<div>⬆️</div>	<div>Branch-HQ-A</div>	<div>🏠</div>	<div>Internet_A (port1)</div>	
<div>⬆️</div>	<div>Branch-HQ-B</div>	<div>🏠</div>	<div>Internet_B (port5)</div>	
<div>⬇️</div>	<div>FGT_AWS_Tun</div>	<div>🏠</div>	<div>Internet_B (port5)</div>	
<div>⬆️</div>	<div>HQ-MPLS</div>	<div>🏠</div>	<div>MPLS-to-HQ (port6)</div>	
<div><div>+ 🏠 Site to Site - FortiGate 1</div></div>				
<div><div>+ 🏠 Dialup - FortiGate 1</div></div>				

Configuring SD-WAN interfaces

In order for us to steer traffic based on SD-WAN rules, first we need to configure SD-WAN interface members. To know more about creating SD-WAN interfaces, refer to the [Configuring the SD-WAN interface on page 452](#) section.

In our example, we created four SD-WAN interface members. SD-WAN interfaces `Internet_A (port1)` and `Internet_B (port5)` for the underlay traffic, and `Branch-HQ-A` and `Branch-HQ-B` interfaces for the overlay traffic.









Verify the configurations on the `Network > SD-WAN` screen:

SD-WAN Interface Members

+ Create New

Edit

Delete

Interfaces	Gateway	Cost	Status
 Internet_A (port1)	10.100.64.254	0	 Enable
 Internet_B (port5)	10.100.65.254	10	 Enable
 VPN_A_Tunnel (Branch-HQ-A)	0.0.0.0	0	 Enable
 VPN_B_Tunnel (Branch-HQ-B)	0.0.0.0	0	 Enable



In the screenshot above, we have configured the `Internet_A (port1)` and `Internet_B (port5)` SD-WAN interface members with their *Cost* values being 0 and 10 respectively. A lower *Cost* value indicates that this member is the primary interface member, and is preferred more than a member with a higher *Cost* value when using the *Lowest Cost (SLA)* strategy.

We also need to configure a static route that points to the *SD-WAN* interface. To know more about static routes, refer to the [Adding a static route on page 454](#) section.

Configuring firewall policies

Configure firewall policies for both the overlay and underlay traffic. To know more about firewall policies, refer to the [Policies on page 767](#) section.

In this example, the *Overlay-out* policy governs the overlay traffic and the *SD-WAN-Out* policy governs the underlay traffic. The firewall policies are configured accordingly.

Once created, verify the firewall policies by navigating to *Policy & Objects > Firewall Policy*:

+ Create New Edit Delete Policy Lookup <input type="text" value="Search"/> <input type="button" value="Q"/> Interface Pair View By Sequence										
ID	Name	From	To	Source	Dest...	Schedule	Service	Action	NAT	Security Profiles
33	SD-WAN-Out	ISFW (port3)	Internet_A (port1) Internet_B (port5)	all	all	always	ALL	ACCEPT	Enabled	<div>APP default</div> <div>SSL certificate-inspection</div>
34	Overlay-out	ISFW (port3)	VPN_A_Tunnel (Branch-HQ-A) VPN_B_Tunnel (Branch-HQ-B)	all	all	always	ALL	ACCEPT	Enabled	<div>SSL no-inspection</div>

The *Security Profiles* column indicates that the *Overlay-out* firewall policy for the overlay traffic is set up to not scan any traffic, while the *SD-WAN-Out* firewall policy is set to scan all web traffic to identify and govern social media traffic as *Application Control* profile is active.

Configuring Performance SLA test

Configure a performance SLA test that will be tied to the SD-WAN interface members we created and assigned to SD-WAN zones. To know more about Performance SLA, refer to the [Performance SLA - SLA targets on page 465](#) section.

In this example, we created a *Performance SLA* test *Default_DNS* with `Internet_A (port1)` and `Internet_B (port5)` interface members as participants. We will use the created *Performance SLA* test to steer all web traffic passing through the underlays other than social media traffic based on the *Lowest Cost (SLA)* strategy.

+ Create New Edit Delete <input type="text" value="Search"/> <input type="button" value="Q"/>					
Name	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
IPv4					
Default_DNS	VPN_A_Tunnel (Branch-HQ-A): 0.00% VPN_B_Tunnel (Branch-HQ-B): 0.00% Internet_A (port1): 0.00% Internet_B (port5): 0.00%	VPN_A_Tunnel (Branch-HQ-A): 31.63ms VPN_B_Tunnel (Branch-HQ-B): 31.57ms Internet_A (port1): 31.21ms Internet_B (port5): 31.11ms	VPN_A_Tunnel (Branch-HQ-A): 0.30ms VPN_B_Tunnel (Branch-HQ-B): 0.28ms Internet_A (port1): 0.30ms Internet_B (port5): 0.27ms	5	10

Configuring SD-WAN rules

Configure SD-WAN rules to govern the steering of DSCP tag-based traffic to the appropriate interfaces. Traffic will be steered based on the *Criteria* configured as part of the SD-WAN rules configuration.

In our example, we configured three different SD-WAN rules to govern DSCP tagged traffic. We have one SD-WAN rule each for VoIP traffic, social media traffic (Facebook in this case), and all other web traffic. VoIP traffic is always steered to either of the two overlays - `VPN_A_tunnel (Branch-HQ-A)` or `VPN_B_tunnel (Branch-HQ-B)`. Similarly, social media traffic and other web traffic is always steered to either of the two underlays - `Internet_A (port1)` or `Internet_B (port5)`. The interface that is preferred by the system over another depends upon the *Criteria* configured in the SD-WAN rule definition.

We configured the following SD-WAN rules:

- [SD-WAN rule for VoIP traffic on page 502](#)
- [SD-WAN rule for social media traffic on page 503](#)
- [SD-WAN rule for other web traffic on page 504](#)

SD-WAN rule for VoIP traffic







To configure SD-WAN rule for DSCP tagged VoIP traffic using the CLI:

```
FortiGate # config sys virtual-wan-link
config service
  edit 1
    set name "VoIP-Steer"
    set mode priority
    set tos 0x70
    set tos-mask 0xf0
    set dst "all"
    set health-check "Default_DNS"
    set link-cost-factor jitter
    set priority-members 4 3
  end
```

The `VoIP-Steer` SD-WAN rule configured above governs the DSCP tagged VoIP traffic.

DSCP values commonly are 6-bit binary numbers that are padded with zeros at the end. Therefore, in this example, VoIP traffic with DSCP tag `011100` will become `01110000`. This 8-bit binary number `01110000` is represented in its hexadecimal form `0x70` as the `tos` (Type of Service bit pattern) value. The `tos-mask` (Type of Service evaluated bits) hexadecimal value of `0xf0` (binary `11110000`) is used to check the four most significant bits from the `tos` value in this case. Hence, the first four bits of the `tos` (`0111`) will be used to match the first four bits of the DSCP tag in our policy above. Only the non-zero bit positions are used for comparison and the zero bit positions are ignored from the `tos-mask`.

We used the *Best Quality* strategy to define the *Criteria* to select the preferred interface from the overlays. With the *Best Quality* strategy selected, the interface with the best measured performance is selected. The system prefers the interface with the least *Jitter*.

Outgoing Interfaces	
Strategy	<div>Manual</div> <div>Best Quality</div> <div>Lowest Cost (SLA)</div> <div>Maximize Bandwidth (SLA)</div>
Interface preference	<div>  VPN_B_Tunnel (Branch-HQ-B)  </div> <div>  VPN_A_Tunnel (Branch-HQ-A)  </div> <div>+</div>
Measured SLA	Default_DNS ▼
Quality criteria	Jitter ▼
Status	<div> Enable</div> <div> Disable</div>

To know more about configuring SD-WAN rules with the *Best Quality* strategy, refer to the [SD-WAN rules - best quality on page 472](#) section.

SD-WAN rule for social media traffic




To configure SD-WAN rule for DSCP tagged social media traffic using the CLI:

```
FortiGate # config sys virtual-wan-link
config service
edit 2
set name "Facebook-DSCP-steer"
set tos 0x30
set tos-mask 0xf0
set dst "all"
set priority-members 2
end
```

The Facebook-DSCP-steer SD-WAN rule configured above governs the DSCP tagged social media traffic.

DSCP values commonly are 6-bit binary numbers that are padded with zeros at the end. Therefore, in this example, social media traffic with DSCP tag 001100 will become 00110000. This 8-bit binary number 00110000 is represented in its hexadecimal form 0x30 as the `tos` (Type of Service bit pattern) value. The `tos-mask` (Type of Service evaluated bits) hexadecimal value of 0xf0 (binary 11110000) is used to check the four most significant bits from the `tos` value in this case. Hence, the first four bits of the `tos` (0011) will be used to match the first four bits of the DSCP tag in our policy above. Only the non-zero bit positions are used for comparison and the zero bit positions are ignored from the `tos-mask`.

We used a manual strategy to select the preferred interface from the underlay SD-WAN zone. We manually select the preferred interface as *Internet_B(port5)* to steer all social media traffic to.

Outgoing Interfaces	
Strategy	<div>Manual</div> <div>Best Quality</div> <div>Lowest Cost (SLA)</div> <div>Maximize Bandwidth (SLA)</div>
Interface preference	<div> Internet_B (port5)</div>
Status	<div> Enable</div> <div> Disable</div>

To know more about configuring SD-WAN rules with static application steering with a manual strategy, refer to the [Static application steering with a manual strategy on page 480](#) section.








SD-WAN rule for other web traffic

To configure SD-WAN rule for all other web traffic using the CLI:

```
FortiGate # config sys virtual-wan-link
config service
edit 3
set name "All-traffic"
set mode sla
set dst "all"
config sla
edit "Default_DNS"
set id 1
next
end
set priority-members 1 2
end
```

The All-traffic SD-WAN rule configured above governs all other web traffic.

We used the *Lowest Cost (SLA)* strategy to define the *Criteria* to select the preferred interface from the underlay SD-WAN zone. With the *Lowest Cost (SLA)* strategy selected, the interface that meets the defined *Performance SLA* targets (*Default_DNS* in our case) is selected. When there is a tie, the interface with the lowest assigned *Cost* (*Internet_A* (port1) in our case) is selected.

Outgoing Interfaces	
Strategy	<div>Manual</div> <div>Best Quality</div> <div>Lowest Cost (SLA)</div> <div>Maximize Bandwidth (SLA)</div>
Interface preference	<div> Internet_A (port1) </div> <div> Internet_B (port5) </div> <div>+</div>
Required SLA target	<div>Default_DNS#1 </div> <div>+</div>
Status	<div> Enable</div> <div> Disable</div>

To know more about configuring SD-WAN rules with the *Lowest Cost (SLA)* strategy, refer to the [SD-WAN rules - lowest cost \(SLA\) on page 475](#) section.

Once configured, verify your SD-WAN rules by navigating to *Network > SD-WAN Rules*:

<div> + Create New Edit Delete <input type="text" value="Search"/> </div>							
ID	Name	Source	Destination	Criteria	Members	Performance SLA	Status
IPv4 3							
1	VoIP-Steer		all	Jitter	VPN_B_Tunnel (Branch-HQ-B) VPN_A_Tunnel (Branch-HQ-A)	Default_DNS	Enabled
2	Facebook-DSCP-steer		all		Internet_B (port5)		Enabled
3	All-traffic		all	SLA	Internet_A (port1) Internet_B (port5)	Default_DNS#1	Enabled
Implicit 1							
	sd-wan	all all	all all	Source IP	any		

Results

The following sections show the function of the FortiGate and specifically of secure SD-WAN with respect to DSCP tagged traffic steering, and can be used to confirm that it is setup and running correctly:

- [Verifying the DSCP tagged traffic on FortiGate on page 505](#)
- [Verifying service rules on page 507](#)
- [Verifying steered traffic leaving the required interface on page 508](#)

Verifying the DSCP tagged traffic on FortiGate

To verify the incoming DSCP tagged traffic, we used packet sniffing and converting the sniffed traffic to a desired format. To know more about packet sniffing, refer to the [Using the FortiOS built-in packet sniffer](#) guide on the *Fortinet Knowledge Base*.

For VoIP traffic that is marked with DSCP tag 0x70:

```
FortiGate # diag sniffer packet any '(ip and ip[1] & 0xfc == 0x70)' 6 0 1
```

We used the open-source packet analyzer *Wireshark* to verify that VoIP traffic is tagged with the 0x70 DSCP tag.

The image shows a Wireshark packet capture window titled 'voip-5061-tcp-udp.pcap'. The packet list shows 24 packets. Packet 24 is selected, showing details for an Internet Protocol Version 4 (IPv4) packet. The DSCP field is highlighted with a red box, showing a value of 0x30 (AF32, ECN: Not-ECT). The packet is a UDP packet from 10.100.88.171 to 10.1.0.102, port 65477 to 5061. The packet length is 242 bytes. The packet details pane shows the following structure:

- Frame 1: 242 bytes on wire (1936 bits), 242 bytes captured (1936 bits)
- Ethernet II, Src: Fortinet_00:03:01 (00:09:0f:00:03:01), Dst: 00:00:00:00:00:01 (00:00:00:00:00:01)
- Internet Protocol Version 4, Src: 10.100.88.171, Dst: 10.1.0.102
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - > Differentiated Services Field: 0x70 (DSCP: AF32, ECN: Not-ECT)
 - Total Length: 228
 - Identification: 0x49de (18910)
 - > Flags: 0x0000
 - Fragment offset: 0
 - Time to live: 127
 - Protocol: UDP (17)
 - Header checksum: 0x8345 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 10.100.88.171
 - Destination: 10.1.0.102
 - User Datagram Protocol, Src Port: 65477, Dst Port: 5061
 - Data (200 bytes)

The packet bytes pane shows the raw data: 0000 00 00 00 00 01 00 09 0f 00 03 01 08 00 45 70Ep. The packet list pane shows 111 packets displayed (100.0%).

For web traffic marked with DSCP tag 0x30:

```
FortiGate # diag sniffer packet any '(ip and ip[1] & 0xfc == 0x30)' 6 0 1
```

We used the open-source packet analyzer *Wireshark* to verify that web traffic is tagged with the 0x30 DSCP tag.

The screenshot shows a Wireshark capture of a network session. The packet list at the top shows a series of packets, including a SYN packet (No. 2) and subsequent data packets. The packet details pane for packet 2 is expanded, showing the Differentiated Services Field (DSCP: AF12, ECN: Not-ECT) highlighted with a red box. The packet bytes pane at the bottom shows the hex representation of the packet.

Verifying service rules

The following CLI commands show the appropriate DSCP tags and the corresponding interfaces selected by the SD-WAN rules to steer traffic:

```
FortiGate # diag sys virtual-wan-link service
```

```
Service(1): Address Mode(IPV4) flags=0x0
TOS(0x70/0xf0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(jitter), link-
cost-threshold(10), health-check(Default_DNS)
Service role: standalone
Member sub interface:
Members:
  1: Seq_num(4), alive, jitter: 0.624, selected
  2: Seq_num(3), alive, jitter: 0.643, selected
Dst address:
  0.0.0.0-255.255.255.255
```

```
Service(2): Address Mode(IPV4) flags=0x0
TOS(0x30/0xf0), Protocol(0: 1->65535), Mode(manual)
Service role: standalone
Member sub interface:
Members:
```

```

1: Seq_num(2), alive, selected
Dst address:
0.0.0.0-255.255.255.255

```

```

Service(3): Address Mode(IPV4) flags=0x0
TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla)
Service role: standalone
Member sub interface:
Members:
1: Seq_num(1), alive, sla(0x1), cfg_order(0), cost(0), selected
2: Seq_num(2), alive, sla(0x1), cfg_order(1), cost(10), selected
Dst address:
0.0.0.0-255.255.255.255

```

Verifying steered traffic leaving the required interface

Go to **Dashboard > Top Policies** to confirm that web traffic (port 443) flows through the right underlay interface members, and VoIP traffic flows through the right overlay interface member.

Web traffic leaves either **Interface_A (port1)** or **Interface_B (port5)**.

Summary of


Policy

SD-WAN-Out (33)


Policy Type

Firewall

Source Interface

 ISFW (port3)

Destination Interface

 Internet_A (port1)

Bytes

5.37 MB


Sessions

314

Bandwidth

4.10 kbps

FortiGate

 -cloud-onramp

Sources

















































Destinations

Applications

Web Sites

Web Categories

Sessions

Source	Device	Destination	Application	Protocol	Source Port	Destination Port	Bytes	Packets	Duration (seconds)	Destination Interface
10.100.88.151	 00:09:0f:00:03:01	 40.67.249.232	 Google Ads	TCP	28417	443	36.00 kB	173	21m 15s	 Internet_A (port1)
10.100.88.151	 00:09:0f:00:03:01	 216.58.192.226	 Google Ads	TCP	28454	443	12.65 kB	47	35s	 Internet_A (port1)
10.100.88.151	 00:09:0f:00:03:01	 216.58.192.132	 HTTPS.BROWSER	TCP	28432	443	12.85 kB	89	39s	 Internet_A (port1)
10.100.88.151	 00:09:0f:00:03:01	 13.249.135.106	 HTTPS.BROWSER	TCP	28447	443	13.93 kB	30	36s	 Internet_A (port1)
10.100.88.151	 00:09:0f:00:03:01	 13.249.135.36	 HTTPS.BROWSER	TCP	28485	443	7.75 kB	22	21s	 Internet_A (port1)
10.100.88.161	 00:09:0f:00:03:01	 157.240.2.25	 Facebook	TCP	28449	443	321.46 kB	264	35s	 Internet_B (port1)
10.100.88.151	 00:09:0f:00:03:01	 69.147.64.34	 Yahoo.Services	TCP	28436	443	8.80 kB	28	39s	 Internet_A (port1)
10.100.88.161	 00:09:0f:00:03:01	 157.240.18.19	 Facebook	TCP	28413	443	8.45 kB	33	2m 13s	 Internet_B (port1)
10.100.88.161	 00:09:0f:00:03:01	 157.240.18.174	 Instagram	TCP	28411	443	193.70 kB	267	2m 14s	 Internet_B (port1)
10.100.88.161	 00:09:0f:00:03:01	 69.171.250.63	 Instagram	TCP	28410	443	23.42 kB	58	2m 16s	 Internet_B (port1)
10.100.88.161	 00:09:0f:00:03:01	 69.171.250.63	 Instagram	TCP	28412	443	10.87 kB	40	2m 14s	 Internet_B (port1)
10.100.88.151	 00:09:0f:00:03:01	 23.35.77.98	 LinkedIn	TCP	28450	443	7.46 kB	24	35s	 Internet_A (port1)

VoIP traffic leaves the preferred **VPN_B_Tunnel (Branch-HQ-B)** interface.

Summary of										
Policy	Overlay-out (34)									
Policy Type	Firewall									
Source Interface	ISFW (port3)									
Destination Interface	VPN_B_Tunnel (Branch-HQ-B)									
Bytes	1.84 MB									
Sessions	3									
Bandwidth	221.35 kbps									
FortiGate	cloud-onramp									
Sources	Destinations	Applications	Web Sites	Web Categories	Sessions ▾					
Source	Device	Destination	Application	Protocol	Source Port	Destination Port	Bytes	Packets	Duration (seconds)	Destination Interface
10.100.88.171	00:09:0f:00:03:01	10.1.0.102	TCP/5061	TCP	34779	5061	728 B	14	17s	VPN_B_Tunnel (Branch-HQ-B)
10.100.88.171	00:09:0f:00:03:01	10.1.0.102	UDP/5061	UDP	65477	5061	1.84 MB	8,084	3m 16s	VPN_B_Tunnel (Branch-HQ-B)
10.100.88.171	00:09:0f:00:03:01	10.1.0.102	UDP/5061	UDP	65478	5061	32 B	1	2m 4s	VPN_B_Tunnel (Branch-HQ-B)

Advanced configuration

The following topics provide instructions on SD-WAN advanced configuration:

- [Self-originating traffic on page 509](#)
- [SDN dynamic connector addresses in SD-WAN rules on page 512](#)
- [Forward error correction on VPN overlay networks on page 515](#)
- [Using BGP tags with SD-WAN rules on page 518](#)
- [BGP multiple path support on page 521](#)
- [Controlling traffic with BGP route mapping and service rules on page 523](#)
- [Applying BGP route-map to multiple BGP neighbors on page 530](#)
- [ADVPN and shortcut paths on page 536](#)
- [DSCP matching \(shaping\) on page 549](#)
- [Dual VPN tunnel wizard on page 552](#)
- [SD-WAN with FGCP HA on page 555](#)

See also [Per packet distribution and tunnel aggregation on page 1273](#).

Self-originating traffic



This topic applies to FortiOS 6.2.15. In other versions, self-originating (local-out) traffic behaves differently.

By default, self-originating traffic, such as Syslog, FortiAnalyzer logging, FortiGuard services, remote authentication, and others, relies on routing table lookups to determine the egress interface that is used to initiate the connection. Policy routes generated by SD-WAN rules do not apply to this traffic.

For the following features, self-originating traffic can be configured to use SD-WAN rules or a specific interface:

PING

IPv4 and IPv6 pings can be configured to use SD-WAN rules.

```
execute ping-options use-sdwan {yes | no}
execute ping6-options use-sdwan {yes | no}
```

DNS

DNS and non-management VDOM DNS traffic can use SD-WAN rules or a specific interface:

```
config system {dns | vdom-dns}
    set interface-select-method {auto | sdwan | specify}
    set interface <interface>
end
```

interface-select-method {auto | sdwan | specify}

Select the interface selection method:

- **auto:** Set the outgoing interface automatically (default)
- **sdwan:** Set the interface by SD-WAN or policy routing rules
- **specify:** Set the interface manually.

interface <interface>

Specify the outgoing interface. This option is only available and must be configured when **interface-select-method** is **specify**.

FortiGuard

FortiGuard traffic can use SD-WAN rules or a specific interface:

```
config system fortiguard
    set interface-select-method {auto | sdwan | specify}
    set interface <interface>
end
```

RADIUS

RADIUS, and individual accounting servers, traffic can use SD-WAN rules or a specific interface:

```
config user radius
    edit <name>
        set interface-select-method {auto | sdwan | specify}
        set interface <interface>
        config accounting-server
            edit <name>
                set interface-select-method {auto | sdwan | specify}
                set interface <interface>
            next
        end
    next
end
```

LDAP

LDAP traffic can use SD-WAN rules or a specific interface:

```
config user ldap
    edit <name>
        set interface-select-method {auto | sdwan | specify}
        set interface <interface>
```

```

    next
end

```

TACACS+

TACACS+ traffic can use SD-WAN rules or a specific interface:

```

config user tacacs+
    edit <name>
        set interface-select-method {auto | sdwan | specify}
        set interface <interface>
    next
end

```

Central management

Central management traffic can use SD-WAN rules or a specific interface:

```

config system central-management
    set interface-select-method {auto | sdwan | specify}
    set interface <interface>
end

```

DHCP proxy

DHCP proxy traffic can use SD-WAN rules or a specific interface:

```

config system settings
    set dhcp-proxy-interface-select-method {auto | sdwan | specify}
    set dhcp-proxy-interface <interface>
end

```

dhcp-proxy-interface-select-method {auto | sdwan | specify}

Select the interface selection method:

- **auto:** Set the outgoing interface automatically (default)
- **sdwan:** Set the interface by SD-WAN or policy routing rules
- **specify:** Set the interface manually.

dhcp-proxy-interface <interface>

Specify the outgoing interface. This option is only available and must be configured when `interface-select-method` is `specify`.

DHCP relay

DHCP relay traffic can use SD-WAN rules or a specific interface:

```

config system interface
    edit <interface>
        set dhcp-relay-interface-select-method {auto | sdwan | specify}
        set dhcp-relay-interface <interface>
    next
end

```

dhcp-relay-interface-select-method {auto | sdwan | specify}

Select the interface selection method:

- **auto:** Set the outgoing interface automatically (default)
- **sdwan:** Set the interface by SD-WAN or policy routing rules

- `specify`: Set the interface manually.

dhcp-relay-interface
<interface>

Specify the outgoing interface. This option is only available and must be configured when `interface-select-method` is `specify`.

CA and local certificate renewal with SCEP

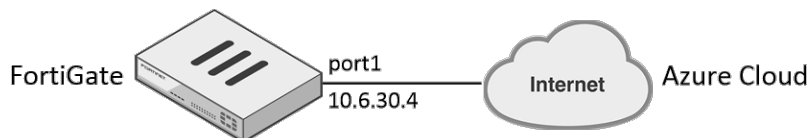
Certificate renewal with SCEP traffic can use SD-WAN rules or a specific interface:

```
config vpn certificate setting
    set interface-select-method {auto | sdwan | specify}
    set interface <interface>
end
```

SDN dynamic connector addresses in SD-WAN rules

SDN dynamic connector addresses can be used in SD-WAN rules. FortiGate supports both public (AWS, Azure, GCP, OCI, AliCloud) and private (Kubernetes, VMware ESXi and NSX, OpenStack, ACI, Nuage) SDN connectors.

The configuration procedure for all of the supported SDN connector types is the same. This example uses an Azure public SDN connector.



There are four steps to create and use an SDN connector address in an SD-WAN rule:

1. Configure the FortiGate IP address and network gateway so that it can reach the Internet.
2. [Create an Azure SDN connector](#).
3. [Create a firewall address to associate with the configured SDN connector](#).
4. [Use the firewall address in an SD-WAN service rule](#).

To create an Azure SDN connector:

1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New*.
3. In the *Public SDN* section, click *Microsoft Azure*.

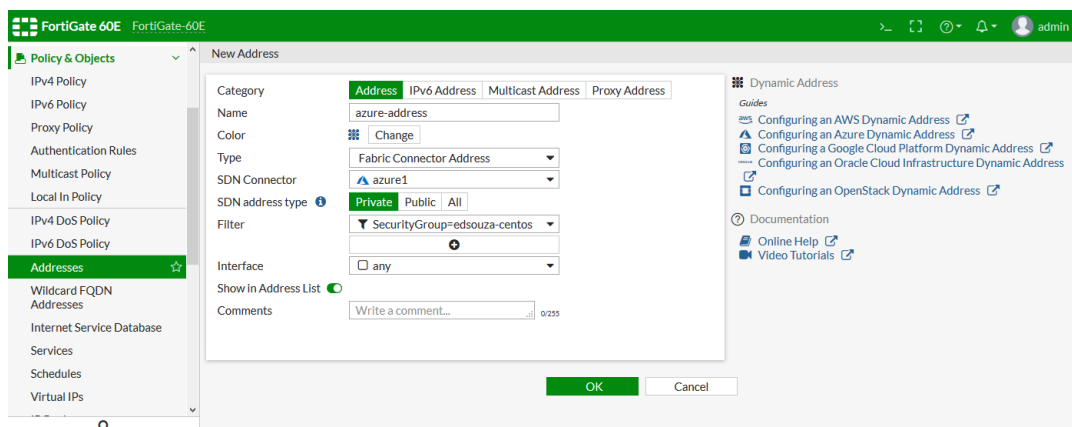
4. Enter the following:

Name	azure1
Status	Enabled
Update Interval	Use Default
Server region	Global
Tenant ID	942b80cd-1b14-42a1-8dcf-4b21dece61ba
Client ID	14dbd5c5-307e-4ea4-8133-68738141feb1
Client secret	xxxxxx
Resource path	disabled

5. Click *OK*.**To create a firewall address to associate with the configured SDN connector:**

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address*.
3. Enter the following:

Category	Address
Name	azure-address
Type	Fabric Connector Address
SDN Connector	azure1
SDN address type	Private
Filter	SecurityGroup=edsouza-centos
Interface	Any

4. Click *OK*.

To use the firewall address in an SD-WAN service rule:

1. Go to *Network > SD-WAN Rules*.
2. Click *Create New*.
3. Set the *Name* to *Azure1*.
4. For the *Destination Address* select *azure-address*.
5. Configure the remaining settings as needed. See [WAN path control on page 463](#) for details.
6. Click *OK*.

Diagnostics

Use the following CLI commands to check the status of and troubleshoot the connector.

To see the status of the SDN connector:

```
diagnose sys sdn status
```

SDN Connector	Type	Status	Updating	Last update
-----	-----	-----	-----	-----
azure1	azure	connected	no	n/a

To debug the SDN connector to resolve the firewall address:

```
diagnose debug application azd -1
```

Debug messages will be on for 30 minutes.

```
...
```

```
azd sdn connector azure1 start updating IP addresses
```

```
azd checking firewall address object azure-address-1, vd 0
```

```
IP address change, new list:
```

```
10.18.0.4
```

```
10.18.0.12
```

```
...
```

```
...
```

```
diagnose sys virtual-wan-link service
```

```
Service(2): Address Mode(IPV4) flags=0x0
```

```
TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
```

```
Service role: standalone
```

```
Member sub interface:
```

```
Members:
```

```
1: Seq_num(1), alive, selected
```

```
Dst address:
```

```
10.18.0.4 - 10.18.0.4
```

```
10.18.0.12 - 10.18.0.12
```

```
... ..
```

```
... ..
```

```
... ..
```


Forward error correction on VPN overlay networks

This topic shows an SD-WAN with forward error correction (FEC) on VPN overlay networks. FEC is a technique used to control and correct errors in data transmission by sending redundant data across the VPN. It uses six parameters in IPsec phase1/phase1-interface settings:

<code>fec-ingress</code>	Enable/disable Forward Error Correction for ingress IPsec traffic (default = disable).
<code>fec-egress</code>	Enable/disable Forward Error Correction for egress IPsec traffic (default = disable).
<code>fec-base</code>	The number of base Forward Error Correction packets (1 - 100, default = 20).
<code>fec-redundant</code>	The number of redundant Forward Error Correction packets (1 - 100, default = 10).
<code>fec-send-timeout</code>	The time before sending Forward Error Correction packets, in milliseconds (1 - 1000, default = 8).
<code>fec-receive-timeout</code>	The time before dropping Forward Error Correction packets, in milliseconds (1 - 1000, default = 5000).

For every `fec-base` number of sent packets, the tunnel will send `fec-redundant` number of redundant packets.

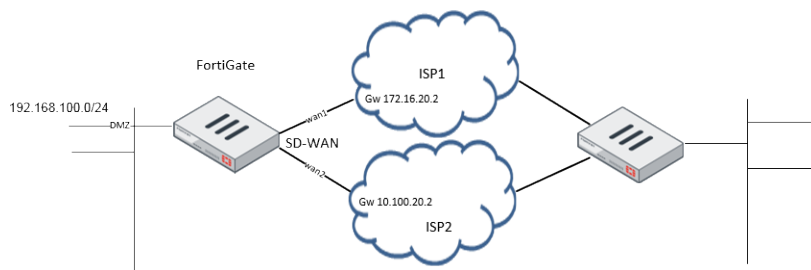
If your FortiGate is NPU capable, disable `npu-offload` in your phase1 configurations:



```
config vpn ipsec phase1-interface
    edit <name>
        set npu-offload disable
    next
end
```

Example

For example, a customer has two ISP connections, wan1 and wan2. Using these two connections, create two IPsec VPN interfaces as SD-WAN members. Configure FEC on each VPN interface to lower packet loss ratio by re-transmitting the packets using its backend algorithm.



To configure IPsec VPN:

```
config vpn ipsec phase1-interface
    edit "vdl-p1"
        set interface "wan1"
        set peertype any
        set net-device disable
```

```
        set proposal aes256-sha256
        set dhgrp 14
        set remote-gw 172.16.201.2
        set psksecret ftnt1234
        set fec-egress enable
        set fec-send-timeout 8
        set fec-base 20
        set fec-redundant 10
        set fec-ingress enable
        set fec-receive-timeout 5000
    next
    edit "vd1-p2"
        set interface "wan2"
        set peertype any
        set net-device disable
        set proposal aes256-sha256
        set dhgrp 14
        set remote-gw 172.16.202.2
        set psksecret ftnt1234
        set fec-egress enable
        set fec-send-timeout 8
        set fec-base 20
        set fec-redundant 10
        set fec-ingress enable
        set fec-receive-timeout 5000
    next
end
config vpn ipsec phase2-interface
    edit "vd1-p1"
        set phasename "vd1-p1"
    next
    edit "vd1-p2"
        set phasename "vd1-p2"
    next
end
```

To configure the interface:

```
config system interface
    edit "vd1-p1"
        set ip 172.16.211.1 255.255.255.255
        set remote-ip 172.16.211.2 255.255.255.255
    next
    edit "vd1-p2"
        set ip 172.16.212.1 255.255.255.255
        set remote-ip 172.16.212.2 255.255.255.255
    next
end
```

To configure the firewall policy:

```
config firewall policy
    edit 1
        set name "1"
        set srcintf "dmz"
        set dstintf ""virtual-wan-link""
```

```

        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

To configure SD-WAN:

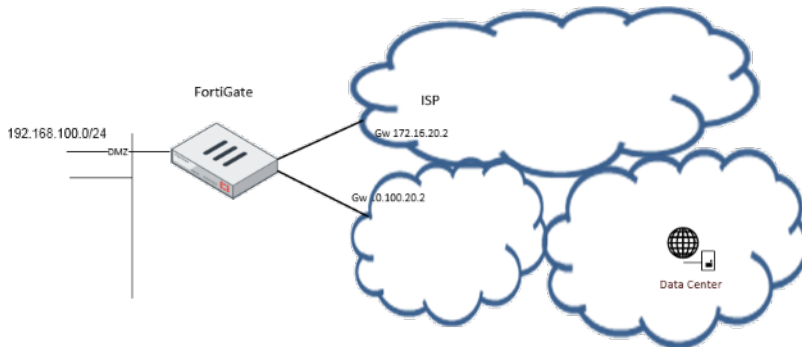
```
config system virtual-wan-link
    set status enable
    config members
        edit 1
            set interface "vd1-p1"
            set gateway 172.16.211.2
        next
        edit 1
            set interface "vd2-p2"
            set gateway 172.16.212.2
        next
    end
end
```

To use the diagnose command to check VPN FEC status:

```
# diagnose vpn tunnel list  
list all ipsec tunnel in vd 0  
-----  
name=vd1 ver=1 serial=1 172.16.200.1:0->172.16.200.2:0  
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/3600 options[0e10]=create_dev  
frag-rtc fec-egress fec-ingress accept_traffic=1  
  
proxyid_num=1 child_num=0 refcnt=11 ilast=8 olast=8 ad=/0  
stat: rxp=0 txp=0 rxb=0 txb=0  
dpd: mode=on-demand on=1 idle=2000ms retry=3 count=0 seqno=0  
natt: mode=None draft=0 interval=0 remote_port=0  
fec-egress: base=20 redundant=10 remote_port=50000 <<<<<<<<<<<<<<<<  
fec-ingress: base=20 redundant=10 <<<<<<<<<<<<<<<<  
proxyid=demo proto=0 sa=1 ref=2 serial=1  
src: 0:10.1.100.0/255.255.255.0:0  
dst: 0:173.1.1.0/255.255.255.0:0  
SA: ref=3 options=10226 type=00 soft=0 mtu=1390 expire=42897/0B replaywin=2048  
seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0  
life: type=01 bytes=0/0 timeout=42899/43200  
dec: spi=181f4f81 esp=aes key=16 6e8fedf2a77691ffdbf3270484cb2555  
ah=sha1 key=20 f92bcf841239d15d30b36b695f78eaef3fad05c4  
enc: spi=0ce10190 esp=aes key=16 2d684fb19cbae533249c8b5683937329  
ah=sha1 key=20 ba7333f89cd34cf75966bd9ffa72030115919213  
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

Using BGP tags with SD-WAN rules

SD-WAN rules can use Border Gateway Protocol (BGP) learned routes as dynamic destinations.



In this example, a customer has two ISP connections, wan1 and wan2. wan1 is used primarily for direct access to internet applications, and wan2 is used primarily for traffic to the customer's data center.

The customer could create an SD-WAN rule using the data center's IP address range as the destination to force that traffic to use wan2, but the data center's IP range is not static. Instead, a BGP tag can be used.

For this example, wan2's BGP neighbor advertises the data center's network range with a community number of 30:5.

This example assumes that SD-WAN is enable on the FortiGate, wan1 and wan2 are added as SD-WAN members, and a policy and static route have been created. See [Configuring the SD-WAN interface on page 452](#) for details.

To configure BGP tags with SD-WAN rules:

1. Configure the community list:

```
config router community-list
  edit "30:5"
    config rule
      edit 1
        set action permit
        set match "30:5"
      next
    end
  next
end
```

2. Configure the route map:

```
config router route-map
  edit "comm1"
    config rule
      edit 1
        set match-community "30:5"
        set set-route-tag 15
      next
    end
  next
end
```

3. Configure BGP:

```
config router bgp
  set as xxxxx
  set router-id xxxx
  config neighbor
    edit "10.100.20.2"
      set soft-reconfiguration enable
      set remote-as xxxxx
      set route-map-in "comm1"
    next
  end
end
```

4. Configure a firewall policy:

```
config firewall policy
  edit 1
    set name "1"
    set srcintf "dmz"
    set dstintf "\"virtual-wan-link\""
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set nat enable
  next
end
```

5. Edit the SD-WAN configuration:

```
config system virtual-wan-link
  set status enable
  config members
    edit 1
      set interface "wan1"
      set gateway 172.16.20.2
    next
    edit 2
      set interface "wan2"
    next
  end
  config service
    edit 1
      set name "DataCenter"
      set mode manual
      set route-tag 15
      set priority-members 2
    next
  end
end
```

Troubleshooting BGP tags with SD-WAN rules**Check the network community**

Use the `get router info bgp network` command to check the network community:

```
# get router info bgp network
BGP table version is 5, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
Network Next Hop Metric LocPrf Weight RouteTag Path
*> 0.0.0.0/0 10.100.1.5 32768 0 ?
*> 1.1.1.1/32 0.0.0.0 32768 0 ?
*> 10.1.100.0/24 172.16.203.2 32768 0 ?
*> 10.100.1.0/30 0.0.0.0 32768 0 ?
*> 10.100.1.4/30 0.0.0.0 32768 0 ?
*> 10.100.1.248/29 0.0.0.0 32768 0 ?
*> 10.100.10.0/24 10.100.1.5 202 10000 15 20 e
*> 172.16.200.0/24 0.0.0.0 32768 0 ?
*> 172.16.200.200/32
      0.0.0.0 32768 0 ?
*> 172.16.201.0/24 172.16.200.4 32768 0 ?
*> 172.16.203.0/24 0.0.0.0 32768 0 ?
*> 172.16.204.0/24 172.16.200.4 32768 0 ?
*> 172.16.205.0/24 0.0.0.0 32768 0 ?
*> 172.16.206.0/24 0.0.0.0 32768 0 ?
*> 172.16.207.1/32 0.0.0.0 32768 0 ?
*> 172.16.207.2/32 0.0.0.0 32768 0 ?
*> 172.16.212.1/32 0.0.0.0 32768 0 ?
*> 172.16.212.2/32 0.0.0.0 32768 0 ?
*> 172.17.200.200/32
      0.0.0.0 32768 0 ?
*> 172.27.1.0/24 0.0.0.0 32768 0 ?
*> 172.27.2.0/24 0.0.0.0 32768 0 ?
*> 172.27.5.0/24 0.0.0.0 32768 0 ?
*> 172.27.6.0/24 0.0.0.0 32768 0 ?
*> 172.27.7.0/24 0.0.0.0 32768 0 ?
*> 172.27.8.0/24 0.0.0.0 32768 0 ?
*> 172.29.1.0/24 0.0.0.0 32768 0 ?
*> 172.29.2.0/24 0.0.0.0 32768 0 ?
*> 192.168.1.0 0.0.0.0 32768 0 ?
```

Total number of prefixes 28

```
# get router info bgp network 10.100.11.0
BGP routing table entry for 10.100.10.0/24
Paths: (2 available, best 1, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
    172.10.22.2
  20
    10.100.20.2 from 10.100.20.2 (6.6.6.6)
      Origin EGP metric 200, localpref 100, weight 10000, valid, external, best
      Community: 30:5 <<<<=====
      Last update: Wen Mar 20 18:45:17 2019
```

Check dynamic BGP addresses

Use the `get router info route-map-address` command to check dynamic BGP addresses:

```
# get router info route-map-address
Extend-tag: 15, interface(wan2:16)
10.100.11.0/255.255.255.0
```

Check dynamic BGP addresses used in policy routes

Use the `diagnose firewall proute list` command to check dynamic BGP addresses used in policy routes:

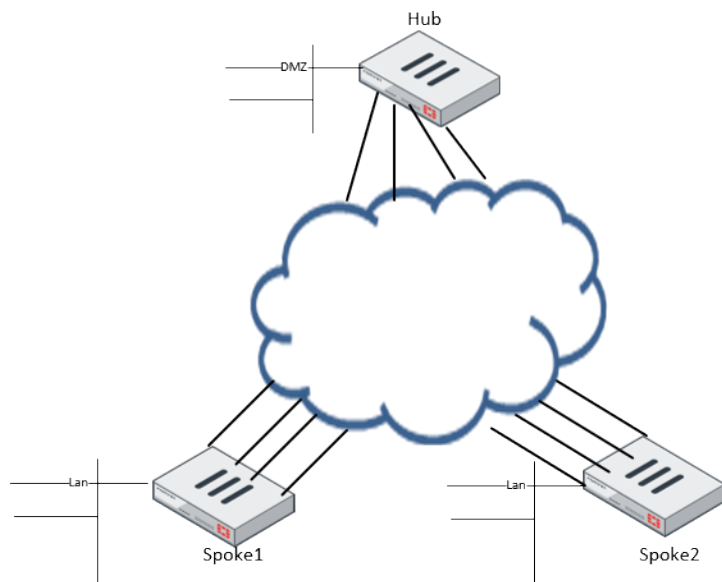
```
# diagnose firewall proute list
list route policy info(vf=root):

id=4278779905 vwl_service=1(DataCenter) flags=0x0 tos=0x00 tos_mask=0x00 protocol=0
sport=0:65535 iif=0 dport=1-65535 oif=16
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 10.100.11.0/255.255.255.0
```

BGP multiple path support

BGP supports multiple paths, allowing an ADVPN to advertise multiple paths. This allows BGP to extend and keep additional network paths according to [RFC 7911](#).

In this example, Spoke1 and Spoke2 each have four VPN tunnels that are connected to the Hub with ADVPN. The Spoke-Hub has established four BGP neighbors on all four tunnels.



Spoke 1 and Spoke 2 can learn four different routes from each other.

To configure the hub:

```
config router bgp
set as 65505
set router-id 11.11.11.11
set ibgp-multipath enable
set additional-path enable
set additional-path-select 4
config neighbor-group
```

```
        edit "gr1"
            set capability-default-originate enable
            set remote-as 65505
            set additional-path both
            set adv-additional-path 4
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.10.0.0 255.255.0.0
            set neighbor-group "gr1"
        next
    end
    config network
        edit 12
            set prefix 11.11.11.11 255.255.255.255
        next
    end
end
```

To configure a spoke:

```
config router bgp
    set as 65505
    set router-id 2.2.2.2
    set ibgp-multipath enable
    set additional-path enable
    set additional-path-select 4
    config neighbor
        edit "10.10.100.254"
            set soft-reconfiguration enable
            set remote-as 65505
            set additional-path both
            set adv-additional-path 4
        next
        edit "10.10.200.254"
            set soft-reconfiguration enable
            set remote-as 65505
            set additional-path both
            set adv-additional-path 4
        next
        edit "10.10.203.254"
            set soft-reconfiguration enable
            set remote-as 65505
            set additional-path both
            set adv-additional-path 4
        next
        edit "10.10.204.254"
            set soft-reconfiguration enable
            set remote-as 65505
            set additional-path both
            set adv-additional-path 4
        next
    end
config network
```



```

        edit 3
            set prefix 22.1.1.0 255.255.255.0
        next
    end
end

```

To view the BGP routing table on a spoke:

```

Spoke1 # get router info routing-table bgp
Routing table for VRF=0
B*   0.0.0.0/0 [200/0] via 10.10.200.254, vd2-2, 03:57:26
      [200/0] via 10.10.203.254, vd2-3, 03:57:26
      [200/0] via 10.10.204.254, vd2-4, 03:57:26
      [200/0] via 10.10.100.254, vd2-1, 03:57:26
B    1.1.1.1/32 [200/0] via 11.1.1.1 (recursive via 12.1.1.1), 03:57:51
      [200/0] via 11.1.1.1 (recursive via 12.1.1.1), 03:57:51
      [200/0] via 11.1.1.1 (recursive via 12.1.1.1), 03:57:51
      [200/0] via 11.1.1.1 (recursive via 12.1.1.1), 03:57:51
B    11.11.11.11/32 [200/0] via 10.10.200.254, vd2-2, 03:57:51
      [200/0] via 10.10.203.254, vd2-3, 03:57:51
      [200/0] via 10.10.204.254, vd2-4, 03:57:51
      [200/0] via 10.10.100.254, vd2-1, 03:57:51
B    33.1.1.0/24 [200/0] via 10.10.204.3, vd2-4, 03:57:26
      [200/0] via 10.10.203.3, vd2-3, 03:57:26
      [200/0] via 10.10.200.3, vd2-2, 03:57:26
      [200/0] via 10.10.100.3, vd2-1, 03:57:26
      [200/0] via 10.10.204.3, vd2-4, 03:57:26
      [200/0] via 10.10.203.3, vd2-3, 03:57:26
      [200/0] via 10.10.200.3, vd2-2, 03:57:26
      [200/0] via 10.10.100.3, vd2-1, 03:57:26
      [200/0] via 10.10.204.3, vd2-4, 03:57:26
      [200/0] via 10.10.203.3, vd2-3, 03:57:26
      [200/0] via 10.10.200.3, vd2-2, 03:57:26
      [200/0] via 10.10.100.3, vd2-1, 03:57:26

```

Controlling traffic with BGP route mapping and service rules

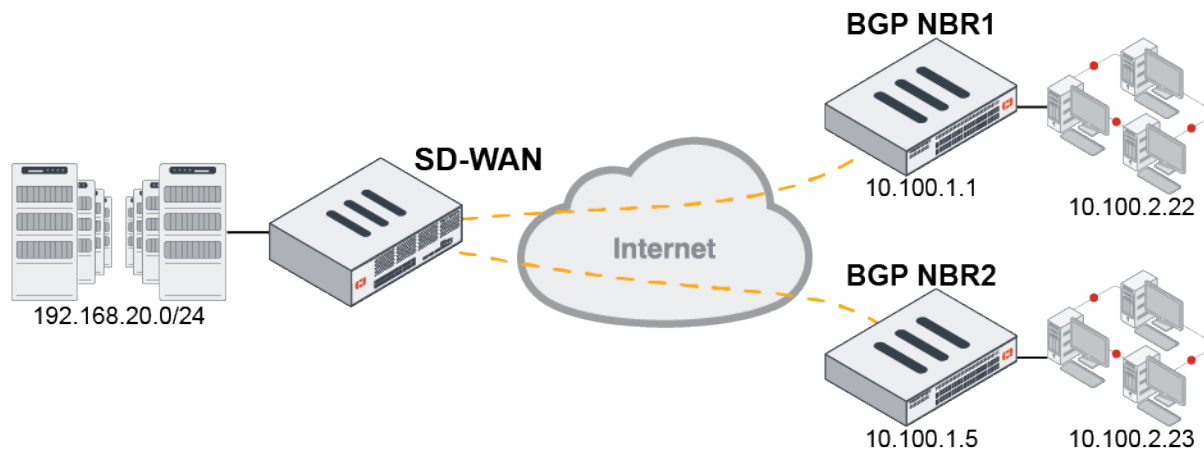
SD-WAN allows you to select different outbound WAN links based on performance SLAs. It is important that BGP neighbors are aware of these settings, and changes to them.

BGP can adapt to changes in SD-WAN link SLAs in the following ways:

- Applying different route-maps based on the SD-WAN's health checks. For example, different BGP community strings can be advertised to BGP neighbors when SLAs are not met.
- Traffic can be selectively forwarded based on the active BGP neighbor. If the SD-WAN service's role matches the active SD-WAN neighbor, the service is enabled. If there is no match, then the service is disabled.

Example

In this topology, a branch FortiGate has two SD-WAN gateways serving as the primary and secondary gateways. The gateways reside in different datacenters, but have a full mesh network between them.



This example shows how route-maps and service rules are selected based on performance SLAs and the member that is currently active. Traffic flows through the primary gateway unless the neighbor's health check is outside of its SLA. If that happens, traffic routes to the secondary gateway.

BGP NBR1 is the primary neighbor and BGP NBR2 is the secondary neighbor.

The branch FortiGate's wan1 and wan2 interfaces are members of the SD-WAN. When the SD-WAN neighbor status is primary, it will advertise community 20:1 to BGP NBR1 and 20:5 to BGP NBR2. When the SD-WAN neighbor status is secondary, it will advertise 20:5 to BGP NBR1 and 20:2 to BGP NBR2.

Only one of the primary or secondary neighbors can be active at one time. The SD-WAN neighbor status is used to decide which neighbor is selected:

- **Primary:** The primary neighbor takes precedence if its SLAs are met.
- **Secondary:** If the primary neighbor's SLAs are not met, the secondary neighbor becomes active if its SLAs are met.
- **Standalone:** If neither the primary or secondary neighbor's SLAs are met, the SD-WAN neighbor status becomes standalone.

Route map

SD-WAN is configured to let BGP advertise different communities when the SLA status changes. When the SLA is missed, it triggers BGP to advertise a different community to its BGP neighbor based on its route-map. The BGP neighbors can use the received community string to select the best path to reach the branch.

To configure BGP route-maps and neighbors:

1. Configure an access for the routes to be matched:

```
config router access-list
  edit "net192"
    config rule
      edit 1
        set prefix 192.168.20.0 255.255.255.0
      next
    next
```

```

        end
    next
end

```

2. Configure the primary neighbor's preferred route-map:

```

config router route-map
    edit "comm1"
        config rule
            edit 1
                set match-ip-address "net192"
                set set-community "20:1"
            next
        end
    next
end

```

3. Configure the secondary neighbor's preferred route-map:

```

config router route-map
    edit "comm2"
        config rule
            edit 1
                set match-ip-address "net192"
                set set-community "20:2"
            next
        end
    next
end

```

4. Configure the failed route-map:

```

config router route-map
    edit "comm5"
        config rule
            edit 1
                set match-ip-address "net192"
                set set-community "20:5"
            next
        end
    next
end

```

5. Configure BGP neighbors:

```

config router bgp
    set as 65412
    set router-id 1.1.1.1
    set ibgp-multipath enable
    config neighbor
        edit "10.100.1.1"
            set soft-reconfiguration enable
            set remote-as 20
            set route-map-out "comm5"
            set route-map-out-preferable "comm1"
        next
        edit "10.100.1.5"
            set soft-reconfiguration enable
            set remote-as 20

```

```
        set route-map-out "comm5"
        set route-map-out-preferable "comm2"
    next
end
end
```

When SLAs are met, `route-map-out-preferable` is used. When SLAs are missed, `route-map-out` is used.

To configure SD-WAN:

1. Configure the SD-WAN members:

```
config system virtual-wan-link
    set status enable
    config members
        edit 1
            set interface "port1"
        next
        edit 2
            set interface "port2"
        next
    end
end
```

2. Configure health checks for each member:

```
config system virtual-wan-link
    config health-check
        edit "ping"
            set server "10.100.2.22"
            set members 1
            config sla
                edit 1
                    set link-cost-factor packet-loss
                    set packetloss-threshold 1
                next
            end
        next
        edit "ping2"
            set server "10.100.2.23"
            set members 2
            config sla
                edit 1
                    set link-cost-factor packet-loss
                    set packetloss-threshold 1
                next
            end
        next
    end
end
```

3. Configure the SD-WAN neighbors and assign them a role and the health checks used to determine if the neighbor meets the SLA:

SD-WAN neighbors can only be configured in the CLI.

```
config system virtual-wan-link
    config neighbor
        edit "10.100.1.1"
```

```
        set member 1
        set role primary
        set health-check "ping"
        set sla-id 1
    next
    edit "10.100.1.5"
        set member 2
        set role secondary
        set health-check "ping2"
        set sla-id 1
    next
end
end
```

Service rules

Create SD-WAN service rules to direct traffic to the primary neighbor when its SLAs are met, and to the secondary neighbor when the primary neighbor's SLAs are missed.

To configure the SD-WAN service rules:

```
config system virtual-wan-link
    config service
        edit 1
            set name "Primary-Out"
            set role primary
            set dst "all"
            set src "all"
            set priority-members 1
        next
        edit 2
            set name "Secondary-Out"
            set role secondary
            set dst "all"
            set src "all"
            set priority-members 2
        next
    end
end
```



If neither the primary nor secondary neighbors are active, the SD-WAN neighbor status becomes standalone. Only service rules with standalone-action enabled will continue to pass traffic. This option is disabled by default.

Verification

To verify when the primary neighbor is passing traffic:

1. Verify the health check status:

```
FortiGate-Branch # diagnose sys virtual-wan-link health-check
Health Check(ping):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(0.569), jitter(0.061) sla_
```

```
map=0x1
Health Check(ping2):
Seq(2 port2): state(alive), packet-loss(0.000%) latency(3.916), jitter(2.373) sla_
map=0x1
```

2. Verify SD-WAN neighbor status:

```
FortiGate-Branch # diagnose sys virtual-wan-link neighbor
SD-WAN neighbor status: hold-down(disable), hold-down-time(0), hold_boot_time(0)
    Selected role(primary) last_secondary_select_time/current_time in seconds 0/572
Neighbor(10.100.1.1): member(1) role(primary)
    Health-check(ping:1) sla-pass selected alive
Neighbor(10.100.1.5): member(2) role(secondary)
    Health-check(ping2:1) sla-pass alive
```

3. Verify service rules status:

```
FortiGate-Branch # diagnose sys virtual-wan-link service

Service(1): Address Mode(IPV4) flags=0x0
    Gen(3), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
    Service role: primary
    Members:
        1: Seq_num(1 port1), alive, selected
    Src address:
        0.0.0.0-255.255.255.255

    Dst address:
        0.0.0.0-255.255.255.255

Service(2): Address Mode(IPV4) flags=0x0
    Gen(6), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
    Service role: secondary, disabled by unselected.
    Members:
        1: Seq_num(2 port2), alive, selected
    Src address:
        0.0.0.0-255.255.255.255

    Dst address:
        0.0.0.0-255.255.255.255
```

4. Verify neighbor routers:

a. Primary neighbor router:

```
FGT-NBR1 # get router info bgp network 192.168.20.0
BGP routing table entry for 192.168.20.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
    Not advertised to any peer
    64512
    10.100.1.2 from 10.100.1.2 (192.168.122.98)
        Origin IGP metric 0, localpref 100, valid, external, best
    Community: 20:1
    Last update: Thu Apr 30 13:41:40 2020
```

b. Secondary neighbor router:

```
FGT-NBR2 # get router info bgp network 192.168.20.0
VRF 0 BGP routing table entry for 192.168.20.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
```

```

Not advertised to any peer
Original VRF 0
64512
10.100.1.6 from 10.100.1.6 (192.168.122.98)
Origin IGP metric 0, localpref 100, valid, external, best
Community: 20:5
Last update: Thu Apr 30 13:41:39 2020

```

To verify when the secondary neighbor is passing traffic:

1. Verify the health check status:

```

FortiGate-Branch # diagnose sys virtual-wan-link health-check
Health Check(ping):
Seq(1 port1): state(dead), packet-loss(54.000%) sla_map=0x0
Health Check(ping2):
Seq(2 port2): state(alive), packet-loss(0.000%) latency(4.339), jitter(3.701) sla_map=0x1

```

2. Verify SD-WAN neighbor status:

```

FortiGate-Branch # diagnose sys virtual-wan-link neighbor
SD-WAN neighbor status: hold-down(disable), hold-down-time(0), hold_boot_time(0)
Selected role(secondary) last_secondary_select_time/current_time in seconds
936/936
Neighbor(10.100.1.1): member(1) role(primary)
Health-check(ping:1) sla-fail dead
Neighbor(10.100.1.5): member(2) role(secondary)
Health-check(ping2:1) sla-pass selected alive

```

3. Verify service rules status:

```

FortiGate-Branch # diagnose sys virtual-wan-link service

Service(1): Address Mode(IPV4) flags=0x0
Gen(4), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Service role: primary, disabled by unselected.
Members:
1: Seq_num(1 port1), alive, selected
Src address:
0.0.0.0-255.255.255.255

Dst address:
0.0.0.0-255.255.255.255

Service(2): Address Mode(IPV4) flags=0x0
Gen(7), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Service role: secondary
Members:
1: Seq_num(2 port2), alive, selected
Src address:
0.0.0.0-255.255.255.255

Dst address:
0.0.0.0-255.255.255.255

```

4. Verify neighbor routers:

a. Primary neighbor router:

```
FGT-NBR1 # get router info bgp network 192.168.20.0
BGP routing table entry for 192.168.20.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  64512
    10.100.1.2 from 10.100.1.2 (192.168.122.98)
      Origin IGP metric 0, localpref 100, valid, external, best
      Community: 20:5
      Last update: Thu Apr 30 15:41:58 2020
```

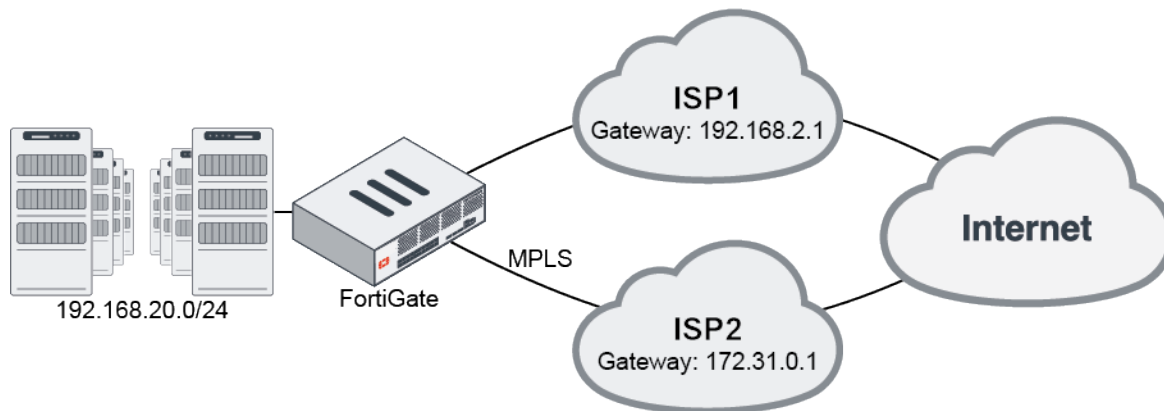
b. Secondary neighbor router:

```
FGT-NBR2 # get router info bgp network 192.168.20.0
VRF 0 BGP routing table entry for 192.168.20.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Original VRF 0
  64512
    10.100.1.6 from 10.100.1.6 (192.168.122.98)
      Origin IGP metric 0, localpref 100, valid, external, best
      Community: 20:2
      Last update: Thu Apr 30 15:42:07 2020
```

Applying BGP route-map to multiple BGP neighbors

[Controlling traffic with BGP route mapping and service rules](#) explained how BGP can apply different route-maps to the primary and secondary SD-WAN neighbors based on SLA health checks.

In this example, SD-WAN neighbors that are not bound to primary and secondary roles are configured.



The FortiGate has multiple SD-WAN links and has formed BGP neighbors with both ISPs.

ISP1 is used primarily for outbound traffic, and has an SD-WAN service rule using the lowest cost algorithm applied to it. When SLAs for ISP1 are not met, it will fail over to the MPLS line.

Inbound traffic is allowed by both WAN links, with each WAN advertising a community string when SLAs are met. When SLAs are not met, the WAN links advertise a different community string.

This example uses two SD-WAN links. The topology can be expanded to include more links as needed.

To configure BGP route-maps and neighbors:**1. Configure an access list for routes to be matched:**

```
config router access-list
  edit "net192"
    config rule
      edit 1
        set prefix 192.168.20.0 255.255.255.0
      next
    end
  next
end
```

2. Configure route-maps for neighbor ISP1:

```
config router route-map
  edit "comm1"
    config rule
      edit 1
        set match-ip-address "net192"
        set set-community "64511:1"
      next
    end
  next
  edit "comm-fail1"
    config rule
      edit 1
        set match-ip-address "net192"
        set set-community "64511:5"
      next
    end
  next
end
```

3. Configure route-maps for neighbor ISP2:

```
config router route-map
  edit "comm2"
    config rule
      edit 1
        set match-ip-address "net192"
        set set-community "64522:1"
      next
    end
  next
  edit "comm-fail2"
    config rule
      edit 1
        set match-ip-address "net192"
        set set-community "64522:5"
      next
    end
  next
end
```

4. Configure the BGP neighbors:

```
config router bgp
  set as 64512
  set keepalive-timer 1
  set holdtime-timer 3
  config neighbor
    edit "192.168.2.1"
      set soft-reconfiguration enable
      set remote-as 64511
      set route-map-out "comm-fail1"
      set route-map-out-preferable "comm1"
    next
    edit "172.31.0.1"
      set soft-reconfiguration enable
      set remote-as 64522
      set route-map-out "comm-fail2"
      set route-map-out-preferable "comm2"
    next
  end
  config network
    edit 1
      set prefix 192.168.20.0 255.255.255.0
    next
  end
end
```

When SLAs are met, `route-map-out-preferable` is used. When SLAs are missed, `route-map-out` is used.

To configure SD-WAN:**1. Configure the SD-WAN members:**

```
config system virtual-wan-link
  set status enable
  config members
    edit 1
      set interface "port1"
      set gateway 192.168.2.1
    next
    edit 2
      set interface "MPLS"
      set cost 20
    next
  end
end
```

2. Configure the health checks that must be met:

```
config system virtual-wan-link
  config health-check
    edit "pingserver"
      set server "8.8.8.8"
      set members 2 1
      config sla
        edit 1
          set link-cost-factor packet-loss
          set packetloss-threshold 2
```

```
        next
      end
    next
  end
end
```

3. Configure the SD-WAN neighbors and assign them a role and the health checks used to determine if the neighbor meets the SLA:

When no role is defined, the default role, `standalone`, is used.

```
config system virtual-wan-link
  config neighbor
    edit "192.168.2.1"
      set member 1
      set health-check "pingserver"
      set sla-id 1
    next
    edit "172.31.0.1"
      set member 2
      set health-check "pingserver"
      set sla-id 1
    next
  end
end
```

Service rules

Create SD-WAN service rules to direct traffic to the SD-WAN links based on the lowest cost algorithm. The same SLA health check and criteria that are used for the SD-WAN neighbor are used for this SD-WAN service rule.

When no roles are defined in the service rule, the default role, `standalone`, is used.

To configure the SD-WAN service rule:

```
config system virtual-wan-link
  config service
    edit 1
      set name "OutboundAll"
      set mode sla
      set dst "all"
      set src "all"
      config sla
        edit "pingserver"
          set id 1
        next
      end
      set priority-members 1 2
    next
  end
end
```

Verification

To verify that when both SLAs are met, port1 is selected due to its lower cost:

1. Verify the health check status:

```
FortiGate-Branch # diagnose sys virtual-wan-link health-check
Health Check(pingserver):
Seq(2 MPLS): state(alive), packet-loss(0.000%) latency(24.709), jitter(14.996) sla_
map=0x1
Seq(1 port1): state(alive), packet-loss(0.000%) latency(28.771), jitter(14.840) sla_
map=0x1
```

2. Verify SD-WAN neighbor status:

```
FortiGate-Branch # diagnose sys virtual-wan-link neighbor
Neighbor(192.168.2.1): member(1) role(standalone)
Health-check(pingserver:1) sla-pass selected alive
Neighbor(172.31.0.1): member(2) role(standalone)
Health-check(pingserver:1) sla-pass selected alive
```

3. Verify service rules status:

Because the service role is standalone, it matches both neighbors. The mode (SLA) determines that port1 is lower cost.

```
FortiGate-Branch # diagnose sys virtual-wan-link service

Service(1): Address Mode(IPV4) flags=0x0
Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
Service role: standalone
Members:
1: Seq_num(1 port1), alive, sla(0x1), cfg_order(0), cost(0), selected
2: Seq_num(2 MPLS), alive, sla(0x1), cfg_order(1), cost(20), selected
Src address:
0.0.0.0-255.255.255.255

Dst address:
0.0.0.0-255.255.255.255
```

4. Verify neighbor routers:

a. Primary neighbor router:

```
FGT-NBR1 # get router info bgp network 192.168.20.0
BGP routing table entry for 192.168.20.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Not advertised to any peer
64512
192.168.2.5 from 192.168.2.5 (192.168.122.98)
Origin IGP metric 0, localpref 100, valid, external, best
Community: 64511:1
Last update: Thu Apr 30 23:59:05 2020
```

b. Secondary neighbor router:

```
FGT-NBR2 # get router info bgp network 192.168.20.0
VRF 0 BGP routing table entry for 192.168.20.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Not advertised to any peer
Original VRF 0
```

```

64512
172.31.0.2 from 172.31.0.2 (192.168.122.98)
  Origin IGP metric 0, localpref 100, valid, external, best
  Community: 64522:1
  Last update: Fri May 1 00:11:28 2020

```

To verify that when neighbor ISP1 misses SLAs, MPLS is selected and BGP advertises a different community string for ISP1:

1. Verify the health check status:

```

FortiGate-Branch # diagnose sys virtual-wan-link health-check
Health Check(pingserver):
Seq(2 MPLS): state(alive), packet-loss(0.000%) latency(25.637), jitter(17.820) sla_map=0x1
Seq(1 port1): state(dead), packet-loss(16.000%) sla_map=0x0

```

2. Verify SD-WAN neighbor status:

```

FortiGate-Branch # diagnose sys virtual-wan-link neighbor
Neighbor(192.168.2.1): member(1) role(standalone)
  Health-check(pingserver:1) sla-fail dead
Neighbor(172.31.0.1): member(2) role(standalone)
  Health-check(pingserver:1) sla-pass selected alive

```

3. Verify service rules status:

As SLA failed for neighbor ISP1, MPLS is preferred.

```

FortiGate-Branch # diagnose sys virtual-wan-link service

Service(1): Address Mode(IPV4) flags=0x0
  Gen(3), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla), sla-compare-order
  Service role: standalone
  Members:
    1: Seq_num(2 MPLS), alive, sla(0x1), cfg_order(1), cost(20), selected
    2: Seq_num(1 port1), dead, sla(0x0), cfg_order(0), cost(0)
  Src address:
    0.0.0.0-255.255.255.255

  Dst address:
    0.0.0.0-255.255.255.255

```

4. Verify neighbor routers:

The community received on ISP1 is updated.

a. Primary neighbor router:

```

FGT-NBR1 # get router info bgp network 192.168.20.0
BGP routing table entry for 192.168.20.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
64512
192.168.2.5 from 192.168.2.5 (192.168.122.98)
  Origin IGP metric 0, localpref 100, valid, external, best
  Community: 64511:5
  Last update: Fri May 1 00:33:26 2020

```

b. Secondary neighbor router:

```
FGT-NBR2 # get router info bgp network 192.168.20.0
VRF 0 BGP routing table entry for 192.168.20.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Original VRF 0
  64512
    172.31.0.2 from 172.31.0.2 (192.168.122.98)
      Origin IGP metric 0, localpref 100, valid, external, best
      Community: 64522:1
      Last update: Fri May  1 00:22:42 2020
```

ADVPN and shortcut paths

This topic provides an example of how to use SD-WAN and ADVPN together.

ADVPN (Auto Discovery VPN) is an IPsec technology that allows a traditional hub-and-spoke VPN's spokes to establish dynamic, on-demand, direct tunnels between each other to avoid routing through the topology's hub device. The primary advantage is that it provides full meshing capabilities to a standard hub-and-spoke topology. This greatly reduces the provisioning effort for full spoke-to-spoke low delay reachability, and addresses the scalability issues associated with very large fully meshed VPN networks.

If a customer's head office and branch offices all have two or more internet connections, they can build a dual-hub ADVPN network. Combined with SD-WAN technology, the customer can load-balance traffic to other offices on multiple dynamic tunnels, control specific traffic using specific connections, or choose better performance connections dynamically.

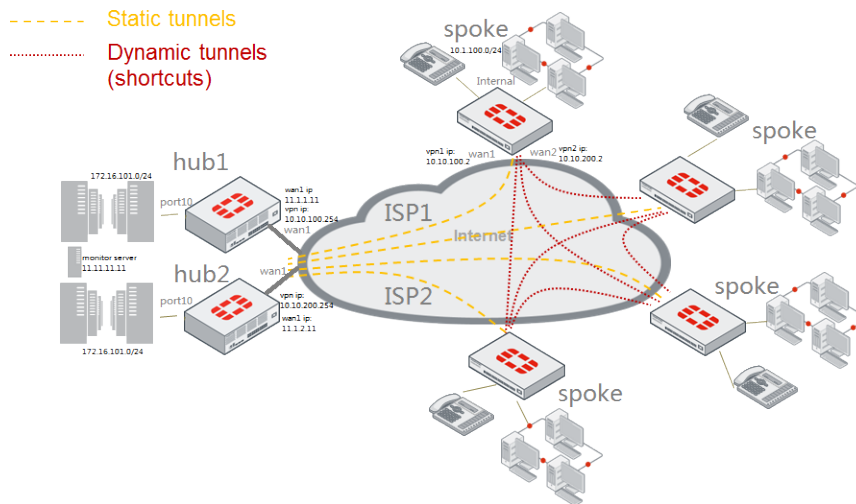


SD-WAN load-balance mode rules (or services) do not support ADVPN members. Other modes' rules, such as SLA and priority, support ADVPN members.

This topic covers three parts:

1. Configure dual-hub ADVPN with multiple branches.
2. Configure BGP to exchange routing information among hubs and spokes.
3. Configure SD-WAN on spoke to do load-balancing and control traffic.

Configuration example



A typical ADVPN configuration with SD-WAN usually has two hubs, and each spoke connects to two ISPs and establishes VPN tunnels with both hubs.

This example shows a hub-and-spoke configuration using two hubs and one spoke:

- Hub1 and Hub2 both use wan1 to connect to the ISPs and port10 to connect to internal network.
- Spoke1 uses wan1 to connect to ISP1 and wan2 to connect to ISP2.
- wan1 sets up VPN to hub1.
- wan2 sets up VPN to hub2.

The SD-WAN is configured on the spoke. It uses the two VPN interfaces as members and two rules to control traffic to headquarters or other spokes using ADVPN VPN interfaces. You can create more rules if required.

For this example:

- Use SD-WAN member 1 (via ISP1) and its dynamic shortcuts for financial department traffic if member 1 meets SLA requirements. If it doesn't meet SLA requirements, it will use SD-WAN member 2 (via ISP2).
- Use SD-WAN member 2 (via ISP2) and its dynamic shortcuts for engineering department traffic.
- Load balance other traffic going to hubs and other spokes between these two members.
- Set up all other traffic to go with their original ISP connection. All other traffic does not go through SD-WAN.
- Set up basic network configuration to let all hubs and spokes connect to their ISPs and the Internet.

Hub internal network	172.16.101.0/24
Spoke1 internal network	10.1.100.0/24
ADVPN 1 network	10.10.100.0/24
ADVPN 2 network	10.10.200.0/24
Hub1 wan1 IP	11.1.1.11
Hub2 wan1 IP	11.1.2.11
Hub1 VPN IP	10.10.100.254
Hub2 VPN IP	10.10.200.254

Spoke1 to hub1 VPN IP	10.10.100.2
Spoke1 to hub2 VPN IP	10.10.200.2
Ping server in Headquarters	11.11.11.11
Internal subnet of spoke1	22.1.1.0/24
Internal subnet of spoke2	33.1.1.0/24
Firewall addresses	Configure hub_subnets and spoke_subnets before using in policies. These can be customized.

The GUI does not support some ADVPN related options, such as auto-discovery-sender, auto-discovery-receiver, auto-discovery-forwarder, and IBGP neighbor-group setting, so this example only provides CLI configuration commands.

Hub1 sample configuration

To configure the IPsec phase1 and phase2 interface:

```
config vpn ipsec phase1-interface
    edit "hub-phase1"
        set type dynamic
        set interface "wan1"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1 3des-
sha1
        set add-route disable
        set dpd on-idle
        set auto-discovery-sender enable
        set tunnel-search nexthop
        set psksecret sample
        set dpd-retryinterval 5
    next
end
config vpn ipsec phase2-interface
    edit "hub-phase2"
        set phase1name "hub-phase1"
        set proposal aes128-sha1 aes256-sha1 3des-sha1 aes128-sha256 aes256-sha256 3des-
sha256
    next
end
```

To configure the VPN interface and BGP:

```
config system interface
    edit "hub-phase1"
        set ip 10.10.100.254 255.255.255.255
        set remote-ip 10.10.100.253 255.255.255.0
    next
end
config router bgp
    set as 65505
    config neighbor-group
        edit "advpn"
```



```
        set link-down-failover enable
        set remote-as 65505
        set route-reflector-client enable
    next
end
config neighbor-range
    edit 1
        set prefix 10.10.100.0 255.255.255.0
        set neighbor-group "advpn"
    next
end
config network
    edit 1
        set prefix 172.16.101.0 255.255.255.0
    next
    edit 2
        set prefix 11.11.11.0 255.255.255.0
    next
end
end
```

To configure the firewall policy:

```
config firewall policy
    edit 1
        set name "spoke2hub"
        set srcintf "hub-phase1"
        set dstintf "port10"
        set srcaddr "spoke_subnets"
        set dstaddr "hub_subnets"
        set action accept
        set schedule "always"
        set service "ALL"
        set comments "allow traffic from spokes to headquater"
    next
    edit 2
        set name "spoke2spoke"
        set srcintf "hub-phase1"
        set dstintf "hub-phase1"
        set srcaddr "spoke_subnets"
        set dstaddr "spoke_subnets"
        set action accept
        set schedule "always"
        set service "ALL"
        set comments "allow traffic from spokes to spokes"
    next
    edit 3
        set name "internal2spoke"
        set srcintf "port10"
        set dstintf "hub-phase1"
        set srcaddr "hub_subnets"
        set dstaddr "spoke_subnets"
        set action accept
        set schedule "always"
        set service "ALL"
        set comments "allow traffic from headquater to spokes"
```

```
    next
end
```

Hub2 sample configuration

Hub2 configuration is the same as hub1 except the wan1 IP address, VPN interface IP address, and BGP neighbor-range prefix.

To configure the IPsec phase1 and phase2 interface:

```
config vpn ipsec phase1-interface
    edit "hub-phase1"
        set type dynamic
        set interface "wan1"
        set peertype any
        set net-device disable
        set proposal aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1 3des-
sha1
        set add-route disable
        set dpd on-idle
        set auto-discovery-sender enable
        set tunnel-search nexthop
        set psksecret sample
        set dpd-retryinterval 5
    next
end
config vpn ipsec phase2-interface
    edit "hub-phase2"
        set phasename "hub-phase1"
        set proposal aes128-sha1 aes256-sha1 3des-sha1 aes128-sha256 aes256-sha256 3des-
sha256
    next
end
```

To configure the VPN interface and BGP:

```
config system interface
    edit "hub-phase1"
        set ip 10.10.200.254 255.255.255.255
        set remote-ip 10.10.200.253 255.255.255.0
    next
end
config router bgp
    set as 65505
    config neighbor-group
        edit "advpn"
            set link-down-failover enable
            set remote-as 65505
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.10.200.0 255.255.255.0
            set neighbor-group "advpn"
```

```
        next
    end
    config network
        edit 1
            set prefix 172.16.101.0 255.255.255.0
        next
        edit 2
            set prefix 11.11.11.0 255.255.255.0
        next
    end
end
```

To configure the firewall policy:

```
config firewall policy
    edit 1
        set name "spoke2hub"
        set srcintf "hub-phase1"
        set dstintf "port10"
        set srcaddr "spoke_subnets"
        set dstaddr "hub_subnets"
        set action accept
        set schedule "always"
        set service "ALL"
        set comments "allow traffic from spokes to headquater"
    next
    edit 2
        set name "spoke2spoke"
        set srcintf "hub-phase1"
        set dstintf "hub-phase1"
        set srcaddr "spoke_subnets"
        set dstaddr "spoke_subnets"
        set action accept
        set schedule "always"
        set service "ALL"
        set comments "allow traffic from spokes to spokes"
    next
    edit 3
        set name "internal2spoke"
        set srcintf "port10"
        set dstintf "hub-phase1"
        set srcaddr "hub_subnets"
        set dstaddr "spoke_subnets"
        set action accept
        set schedule "always"
        set service "ALL"
        set comments "allow traffic from headquater to spokes"
    next
end
```

Spoke1 sample configuration**To configure the IPsec phase1 and phase2 interface:**

```

config vpn ipsec phase1-interface
    edit "spoke1-phase1"
        set interface "wan1"
        set peertype any
        set net-device enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set add-route disable
        set dpd on-idle
        set auto-discovery-receiver enable
        set remote-gw 11.1.1.11
        set psksecret sample
        set dpd-retryinterval 5
    next
    edit "spoke1-2-phase1"
        set interface "wan2"
        set peertype any
        set net-device enable
        set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
        set add-route disable
        set dpd on-idle
        set auto-discovery-receiver enable
        set remote-gw 11.1.2.11
        set psksecret sample
        set dpd-retryinterval 5
    next
end
config vpn ipsec phase2-interface
    edit "spoke1-phase2"
        set phasename "spoke1-phase1"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
chacha20poly1305
        set auto-negotiate enable
    next
    edit "spoke1-2-phase2"
        set phasename "spoke1-2-phase1"
        set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
chacha20poly1305
        set auto-negotiate enable
    next
end

```

To configure the VPN interface and BGP:

```

config system interface
    edit "spoke1-phase1"
        set ip 10.10.100.2 255.255.255.255
        set remote-ip 10.10.100.254 255.255.255.0
    next
    edit "spoke1-2-phase1"
        set ip 10.10.200.2 255.255.255.255
        set remote-ip 10.10.200.254 255.255.255.0
    next
end

```

```
end
config router bgp
  set as 65505
  config neighbor
    edit "10.10.100.254"
      set advertisement-interval 1
      set link-down-failover enable
      set remote-as 65505
    next
    edit "10.10.200.254"
      set advertisement-interval 1
      set link-down-failover enable
      set remote-as 65505
    next
  end
config network
  edit 1
    set prefix 10.1.100.0 255.255.255.0
  next
end
end
```

To configure SD-WAN:

```
config system virtual-wan-link
  set status enable
  config members
    edit 1
      set interface "spoke1-phase1"
    next
    edit 2
      set interface "spoke1-2-phase1"
    next
  end
config health-check
  edit "ping"
    set server "11.11.11.11"
    set members 1 2
    config sla
      edit 1
        set latency-threshold 200
        set jitter-threshold 50
        set packetloss-threshold 5
      next
    end
  end
next
end
config service
  edit 1
    set mode sla
    set dst "finacial-department"
    config sla
      edit "ping"
        set id 1
      next
    end
  end
```

```

        end
        set priority-member 1 2
    next
    edit 2
        set member 2
        set dst "engineering-department"
    next
end
end

```

To configure the firewall policy:

```

config firewall policy
    edit 1
        set name "outbound_advpn"
        set srcintf "internal"
        set dstintf "virtual-wan-link"
        set srcaddr "spoke_subnets"
        set dstaddr "spoke_subnets" "hub_subnets"
        set action accept
        set schedule "always"
        set service "ALL"
        set comments "allow internal traffic going out to headquarter and other spokes"
    next
    edit 2
        set name "inbound_advpn"
        set srcintf "virtual-wan-link"
        set dstintf "internal"
        set srcaddr "spoke_subnets" "hub_subnets"
        set dstaddr "spoke_subnets"
        set action accept
        set schedule "always"
        set service "ALL"
        set comments "allow headquarter and other spokes traffic coming in"
    next
end

```

Troubleshooting ADVPN and shortcut paths

Before spoke vs spoke shortcut VPN is established

Use the following CLI commands to check status before spoke vs spoke shortcut VPN is established.

get router info bgp summary

```

BGP router identifier 2.2.2.2, local AS number 65505
BGP table version is 13
3 BGP AS-PATH entries
0 BGP community entries

```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
10.10.100.254	4	65505	3286	3270	11	0	0	00:02:15	5
10.10.200.254	4	65505	3365	3319	12	0	0	00:02:14	5

```
Total number of neighbors 2
```

get router info routing-table bgp

Routing table for VRF=0

```

B*      0.0.0.0/0 [200/0] via 10.10.200.254, spoke1-2-phasel, 00:00:58
          [200/0] via 10.10.100.254, spoke1-phasel, 00:00:58
B       1.1.1.1/32 [200/0] via 11.1.1.1 (recursive via 12.1.1.1), 00:01:29
          [200/0] via 11.1.1.1 (recursive via 12.1.1.1), 00:01:29
B       11.11.11.0/24 [200/0] via 10.10.200.254, spoke1-2-phasel, 00:01:29
          [200/0] via 10.10.100.254, spoke1-phasel, 00:01:29
B       33.1.1.0/24 [200/0] via 10.10.200.3, spoke1-2-phasel, 00:00:58
          [200/0] via 10.10.100.3, spoke1-phasel, 00:00:58
          [200/0] via 10.10.200.3, spoke1-2-phasel, 00:00:58
          [200/0] via 10.10.100.3, spoke1-phasel, 00:00:58

```

diagnose vpn tunnel list

list all ipsec tunnel in vd 3

```

-----
name=spoke1-phasel ver=1 serial=5 12.1.1.2:0->11.1.1.11:0 dst_mtu=15324
bound_if=48 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu create_dev
frag-rfc accept_traffic=1

```

```

proxyid_num=1 child_num=0 refcnt=22 ilast=0 olast=0 ad=r/2
stat: rxp=1 txp=185 rxb=16428 txb=11111
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=4
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=spoke1 proto=0 sa=1 ref=4 serial=1 auto-negotiate adr
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=6 options=1a227 type=00 soft=0 mtu=15262 expire=42820/0B replaywin=2048
seqno=ba esn=0 replaywin_lastseq=00000002 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42903/43200
dec: spi=03e01a2a esp=aes key=16 56e673f0df05186aa657f55cbb631c13
ah=sha1 key=20 b0d50597d9bed763c42469461b03da8041f87e88
enc: spi=2ead61bc esp=aes key=16 fe0ccd4a3ec19fe6d520c437eb6b8897
ah=sha1 key=20 e3e669bd6df41b88eadaacba66463706f26fb53a
dec:pkts/bytes=1/16368, enc:pkts/bytes=185/22360
npu_flag=03 npu_rgwy=11.1.1.11 npu_lgwy=12.1.1.2 npu_selid=0 dec_npuid=1 enc_npuid=1
-----

```

```

name=spoke1-2-phasel ver=1 serial=6 112.1.1.2:0->11.1.2.11:0 dst_mtu=15324
bound_if=90 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu create_dev
frag-rfc accept_traffic=1

```

```

proxyid_num=1 child_num=0 refcnt=21 ilast=0 olast=0 ad=r/2
stat: rxp=1 txp=186 rxb=16498 txb=11163
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=74
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=spoke1-2 proto=0 sa=1 ref=4 serial=1 auto-negotiate adr
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=6 options=1a227 type=00 soft=0 mtu=15262 expire=42818/0B replaywin=2048
seqno=bb esn=0 replaywin_lastseq=00000002 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42901/43200
dec: spi=03e01a2b esp=aes key=16 fe49f5042a5ad236250bf53312db1346
ah=sha1 key=20 5dbb15c8cbc046c284bb1c6425dac2b3e15bec85
enc: spi=2ead61bd esp=aes key=16 d6d97be52c3cccb9e88f28a9db64ac46
ah=sha1 key=20 e20916ae6ea2295c2fbd5cbc8b8f5dd8b17f52f1

```

```
dec:pkts/bytes=1/16438, enc:pkts/bytes=186/22480
npu_flag=03 npu_rgw=11.1.2.11 npu_lgw=112.1.1.2 npu_selid=1 dec_npuid=1 enc_npuid=1
```

diagnose sys virtual-wan-link service

```
Service(1): Address Mode(IPV4) flags=0x0
TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla)
Member sub interface:
Members:
  1: Seq_num(1), alive, sla(0x1), cfg_order(0), cost(0), selected
  2: Seq_num(2), alive, sla(0x1), cfg_order(1), cost(0), selected
Dst address: 33.1.1.1-33.1.1.100
```

```
Service(2): Address Mode(IPV4) flags=0x0
TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Member sub interface:
Members:
  1: Seq_num(2), alive, selected
Dst address: 33.1.1.101-33.1.1.200
```

diagnose firewall proute list

```
list route policy info(vf=vd2):
```

```
id=2132869121 vwl_service=1 vwl_mbr_seq=1 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_
mask=0x00 protocol=0 sport=0:65535 iif=0 dport=1-65535 oif=70 oif=71
destination(1): 33.1.1.1-33.1.1.100
source wildcard(1): 0.0.0.0/0.0.0.0
```

```
id=2132869122 vwl_service=2 vwl_mbr_seq=2 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_
mask=0x00 protocol=0 sport=0:65535 iif=0 dport=1-65535 oif=71
destination(1): 33.1.1.101-33.1.1.200
source wildcard(1): 0.0.0.0/0.0.0.0
```

After spoke vs spoke shortcut VPN is established

Use the following CLI commands to check status after spoke vs spoke shortcut VPN is established.

get router info routing-table bgp

```
Routing table for VRF=0
B*      0.0.0.0/0 [200/0] via 10.10.200.254, spoke1-2-phase1, 00:01:33
          [200/0] via 10.10.100.254, spoke1-phase1, 00:01:33
B       1.1.1.1/32 [200/0] via 11.1.1.1 (recursive via 12.1.1.1), 00:02:04
          [200/0] via 11.1.1.1 (recursive via 12.1.1.1), 00:02:04
B       11.11.11.0/24 [200/0] via 10.10.200.254, spoke1-2-phase1, 00:02:04
          [200/0] via 10.10.100.254, spoke1-phase1, 00:02:04
B       33.1.1.0/24 [200/0] via 10.10.200.3, spoke1-2-phase1_0, 00:01:33
          [200/0] via 10.10.100.3, spoke1-phase1_0, 00:01:33
          [200/0] via 10.10.200.3, spoke1-2-phase1_0, 00:01:33
          [200/0] via 10.10.100.3, spoke1-phase1_0, 00:01:33
```

diagnose sys virtual-wan-link service

```
Service(1): Address Mode(IPV4) flags=0x0
TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla)
Member sub interface:
  1: seq_num(1), interface(spoke1-phase1):
      1: spoke1-phase1_0(111)
```



```

    2: seq_num(2), interface(spoke1-2-phase1):
        1: spoke1-2-phase1_0(113)
Members:
    1: Seq_num(1), alive, sla(0x1), cfg_order(0), cost(0), selected
    2: Seq_num(2), alive, sla(0x1), cfg_order(1), cost(0), selected
Dst address: 33.1.1.1-33.1.1.100

Service(2): Address Mode(IPV4) flags=0x0
TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Member sub interface:
    1: seq_num(2), interface(spoke1-2-phase1):
        1: spoke1-2-phase1_0(113)
Members:
    1: Seq_num(2), alive, selected
Dst address: 33.1.1.101-33.1.1.200

# diagnose vpn tunnel list
list all ipsec tunnel in vd 3
-----
name=spoke1-phase1 ver=1 serial=5 12.1.1.2:0->11.1.1.11:0 dst_mtu=15324
bound_if=48 lgwy=static/1 tun=intf/0 mode=auto/1 encaps=none/536 options[0218]=npu create_dev
frag-rfc accept_traffic=1

proxyid_num=1 child_num=1 refcnt=20 ilast=0 olast=0 ad=r/2
stat: rxp=1 txp=759 rxb=16428 txb=48627
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=4
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=vd2-1 proto=0 sa=1 ref=5 serial=1 auto-negotiate adr
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=6 options=1a227 type=00 soft=0 mtu=15262 expire=42536/0B replaywin=2048
seqno=2f8 esn=0 replaywin_lastseq=00000002 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42898/43200
dec: spi=03e01a42 esp=aes key=16 1f131bda108d33909d49fc2778bd08bb
ah=sha1 key=20 14131d3f0da9b741a2fd13d530b0553aa1f58983
enc: spi=2ead61d8 esp=aes key=16 81ed24d5cd7bb59f4a80dceb5a560e1f
ah=sha1 key=20 d2ccc2f3223ce16514e75f672cd88c4b4f48b681
dec:pkts/bytes=1/16360, enc:pkts/bytes=759/94434
npu_flag=03 npu_rgwy=11.1.1.11 npu_lgwy=12.1.1.2 npu_selid=0 dec_npuid=1 enc_npuid=1
-----
name=spoke1-2-phase1 ver=1 serial=6 112.1.1.2:0->11.1.2.11:0 dst_mtu=15324
bound_if=90 lgwy=static/1 tun=intf/0 mode=auto/1 encaps=none/536 options[0218]=npu create_dev
frag-rfc accept_traffic=1

proxyid_num=1 child_num=1 refcnt=19 ilast=0 olast=0 ad=r/2
stat: rxp=1 txp=756 rxb=16450 txb=48460
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=74
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=vd2-2 proto=0 sa=1 ref=5 serial=1 auto-negotiate adr
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=6 options=1a227 type=00 soft=0 mtu=15262 expire=42538/0B replaywin=2048
seqno=2f5 esn=0 replaywin_lastseq=00000002 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42900/43200
dec: spi=03e01a43 esp=aes key=16 7fc87561369f88b56d08bfda769eb45b
ah=sha1 key=20 0ed554ef231c5ac16dc2e71d1907d7347dda33d6
enc: spi=2ead61d9 esp=aes key=16 00286687aa1762e7d8216881d6720ef3

```

```

    ah=sha1 key=20 59d5eec6299ebcf038c190860774e2833074d7c3
    dec:pkts/bytes=1/16382, enc:pkts/bytes=756/94058
    npu_flag=03 npu_rgw=11.1.2.11 npu_lgw=112.1.1.2 npu_selid=1 dec_npuid=1 enc_npuid=1
-----
name=spoke1-phasel_0 ver=1 serial=55 12.1.1.2:0->13.1.1.3:0 dst_mtu=15324
bound_if=48 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/728 options[02d8]=npu
create_dev no-sysctl rgwy-chg frag-rfc accept_traffic=1

parent=vd2-1 index=0
proxyid_num=1 child_num=0 refcnt=18 ilast=8 olast=8 ad=r/2
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=vd2-1 proto=0 sa=1 ref=2 serial=1 auto-negotiate adr
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=3 options=1a227 type=00 soft=0 mtu=15262 expire=42893/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42901/43200
dec: spi=03e01a44 esp=aes key=16 c3b77a98e3002220e2373b73af14df6e
ah=sha1 key=20 d18d107c248564933874f60999d6082fd7a78948
enc: spi=864f6dba esp=aes key=16 eb6181806ccb9bac37931f9eadd4d5eb
ah=sha1 key=20 ab788f7a372877a5603c4ede1be89a592fc21873
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
npu_flag=00 npu_rgw=13.1.1.3 npu_lgw=12.1.1.2 npu_selid=51 dec_npuid=0 enc_npuid=0
-----
name=spoke1-2-phasel_0 ver=1 serial=57 112.1.1.2:0->113.1.1.3:0 dst_mtu=15324
bound_if=90 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/728 options[02d8]=npu
create_dev no-sysctl rgwy-chg frag-rfc accept_traffic=1

parent=vd2-2 index=0
proxyid_num=1 child_num=0 refcnt=17 ilast=5 olast=5 ad=r/2
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=vd2-2 proto=0 sa=1 ref=3 serial=1 auto-negotiate adr
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=3 options=1a227 type=00 soft=0 mtu=15262 expire=42900/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42901/43200
dec: spi=03e01a45 esp=aes key=16 0beb519ed9f800e8b4c0aa4e1df7da35
ah=sha1 key=20 bc9f38db5296cce4208a69f1cc8a9f7ef4803c37
enc: spi=864f6dbb esp=aes key=16 1d26e3556afcdb9f8e3e33b563b44228
ah=sha1 key=20 564d05ef6f7437e1fd0a88d5fee7b6567f9d387e
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
npu_flag=00 npu_rgw=113.1.1.3 npu_lgw=112.1.1.2 npu_selid=53 dec_npuid=0 enc_npuid=0

# diagnose firewall proute list
list route policy info(vf=vd2):

id=2132869121 vwl_service=1 vwl_mbr_seq=1 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_
mask=0x00 protocol=0 sport=0:65535 iif=0 dport=1-65535 oif=111 oif=70 oif=113 oif=71
destination(1): 33.1.1.1-33.1.1.100
source wildcard(1): 0.0.0.0/0.0.0.0

id=2132869122 vwl_service=2 vwl_mbr_seq=2 dscp_tag=0xff 0xff flags=0x0 tos=0x00 tos_

```

```
mask=0x00 protocol=0 sport=0:65535 iif=0 dport=1-65535 oif=113 oif=71
destination(1): 33.1.1.101-33.1.1.200
source wildcard(1): 0.0.0.0/0.0.0.0
```

DSCP matching (shaping)

This feature has three parts:

- [DSCP matching in firewall policies](#)
- [DSCP matching in firewall shaping policies](#)
- [DSCP marking in firewall shaping policies](#)

DSCP matching in firewall policies

Traffic is allowed or blocked according to the DSCP values in the incoming packets.

The following CLI variables are available in the `config firewall policy` command:

<code>tos-mask <mask_value></code>	Non-zero bit positions are used for comparison. Zero bit positions are ignored (default = 0x00). This variable replaces the <code>dscp-match</code> variable.
<code>tos <tos_value></code>	Type of Service (ToC) value that is used for comparison (default = 0x00). This variable is only available when <code>tos-mask</code> is not zero. This variable replaces the <code>dscp-value</code> variable.
<code>tos-negate {enable disable}</code>	Enable/disable negated ToS match (default = disable). This variable is only available when <code>tos-mask</code> is not zero. This variable replaces the <code>dscp-negate</code> variable.

DSCP matching in firewall shaping policies

Shaping is applied to the session or not according to the DSCP values in the incoming packets. The same logic and commands as in firewall policies are used.

DSCP marking in firewall shaping policies

Traffic is allowed or blocked according to the DSCP values in the incoming packets. DSCP marking in firewall shaping policies uses the same logic and commands as in firewall policy and traffic-shaper.

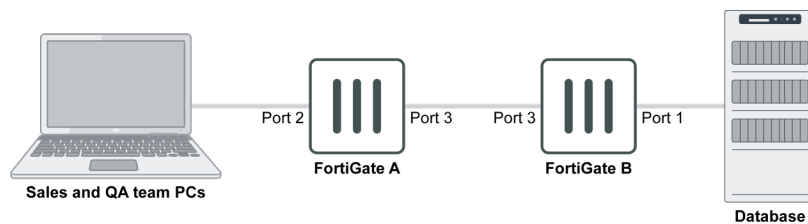
When DSCP marking on `firewall shaper traffic-shaper`, `firewall shaping-policy`, and `firewall policy` all apply to the same session, `shaping-policy` overrides `policy`, and `shaper traffic-shaper` overrides both `shaping-policy` and `policy`.

The following CLI variables in `config firewall policy` are used to mark the packets:

<code>diffserv-forward {enable disable}</code>	Enable/disable changing a packet's DiffServ values to the value specified in <code>diffservcode-forward</code> (default = disable).
<code>diffservcode-forward <dscp_value></code>	The value that packet's DiffServ is set to (default = 000000). This variable is only available when <code>diffserv-forward</code> is enabled.

<code>diffserv-reverse {enable disable}</code>	Enable/disable changing a packet's reverse (reply) DiffServ values to the value specified in <code>diffservcode-rev</code> (default = disable).
<code>diffservcode-rev <dscp_ value></code>	The value that packet's reverse (reply) DiffServ is set to (default = 000000). This variable is only available when <code>diffserv-rev</code> is enabled.

Examples



Example 1

FortiGate A marks traffic from the sales and QA teams with different DSCP values. FortiGate B does DSCP matching, allowing only the sales team to access the database.

1. Configure FortiGate A:

```

config firewall policy
  edit 1
    set srcintf "port2"
    set dstintf "port3"
    set srcaddr "QA"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set diffserv-forward enable
    set diffservcode-forward 110000
    set nat enable
  next

  edit 5
    set srcintf "port2"
    set dstintf "port3"
    set srcaddr "Sales"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set diffserv-forward enable
    set diffservcode-forward 111011
    set nat enable
  next
end

```

2. Configure FortiGate B:

```

config firewall policy
  edit 2

```

```

        set srcintf "port3"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "Database"
        set action accept
        set schedule "always"
        set service "ALL"
        set tos-mask 0xf0
        set tos 0xe0
        set fsso disable
        set nat enable
    next
end

```

Example 2

FortiGate A marks traffic from the sales and QA teams with different DSCP values. FortiGate B uses a firewall shaping policy to do the DSCP matching, limiting the connection speed of the sales team to the database to 10MB/s.

1. Configure FortiGate A:

```

config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port3"
        set srcaddr "QA"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set diffserv-forward enable
        set diffservcode-forward 110000
        set nat enable
    next

    edit 5
        set srcintf "port2"
        set dstintf "port3"
        set srcaddr "Sales"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set diffserv-forward enable
        set diffservcode-forward 111011
        set nat enable
    next
end

```

2. Configure FortiGate B:

```

config firewall policy
    edit 2
        set srcintf "port3"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
    next
end

```

```
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end

config firewall shaper traffic-shaper
    edit "10MB/s"
        set guaranteed-bandwidth 60000
        set maximum-bandwidth 80000
    next
end

config firewall shaping-policy
    edit 1
        set service "ALL"
        set dstintf "port1"
        set tos-mask 0xf0
        set tos 0xe0
        set traffic-shaper "10MB/s"
        set srcaddr "all"
        set dstaddr "all"
    next
end
```

Example 3

FortiGate A has a traffic shaping policy to mark traffic from the QA team with a DSCP value of 100000, while reverse traffic is marked with 000011.

1. Configure FortiGate A:

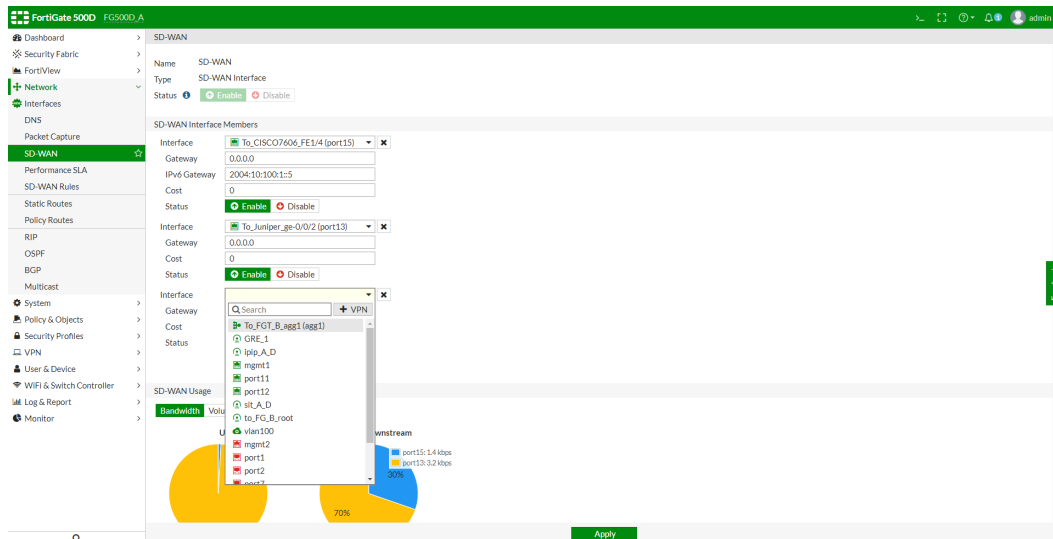
```
config firewall shaping-policy
    edit 1
        set name "QA Team 50MB"
        set service "ALL"
        set dstintf "port3"
        set traffic-shaper "50MB/s"
        set traffic-shaper-reverse "50MB/s"
        set diffserv-forward enable
        set diffserv-reverse enable
        set srcaddr "QA"
        set dstaddr "all"
        set diffservcode-forward 100000
        set diffservcode-rev 000011
    next
end
```

Dual VPN tunnel wizard

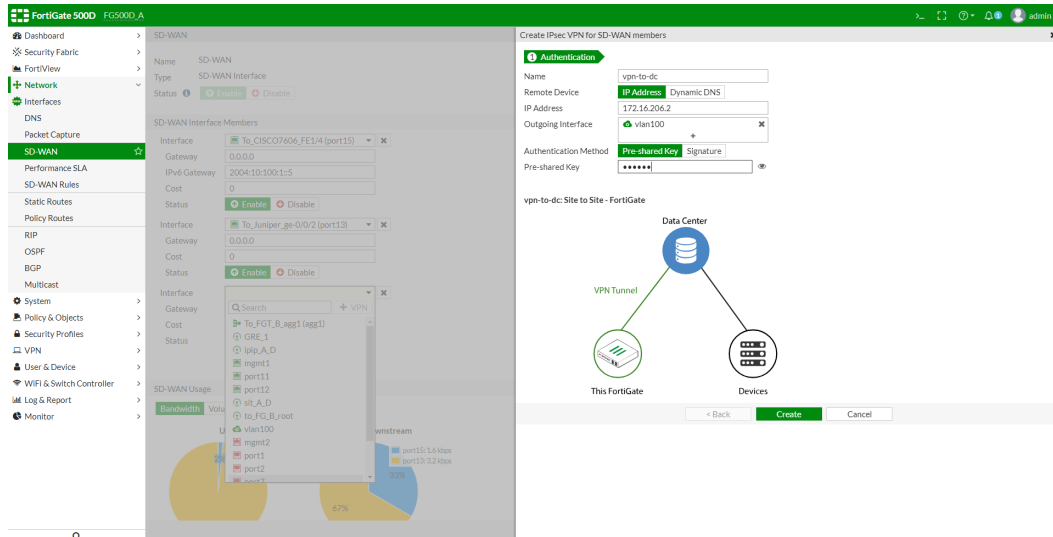
This wizard is used to automatically set up multiple VPN tunnels to the same destination over multiple outgoing interfaces. This includes automatically configuring IPsec, routing, and firewall settings, avoiding cumbersome and error-prone configuration steps.

To create a new SD-WAN VPN interface using the tunnel wizard:

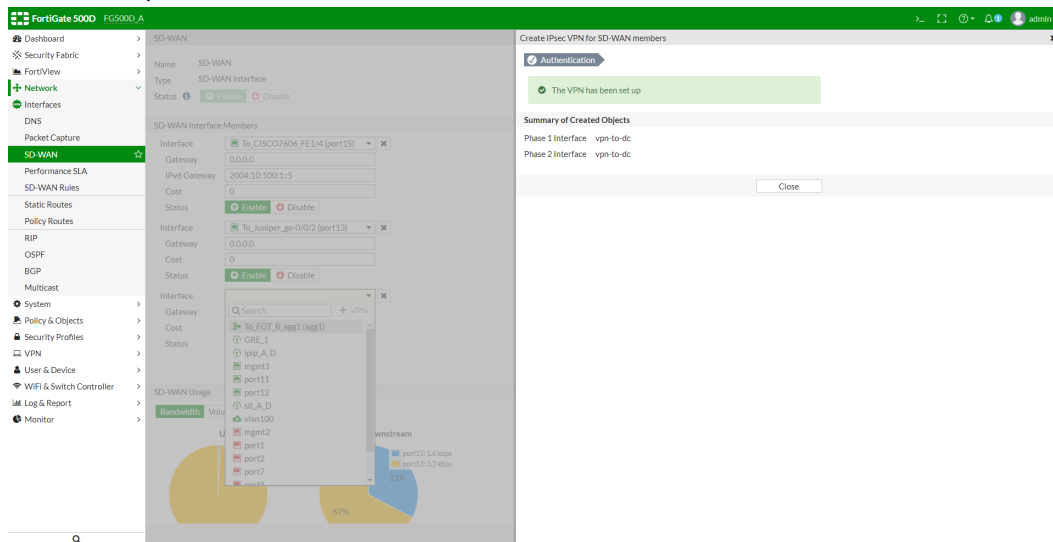
1. Go to *Network > SD-WAN*.
2. Add a new interface member.



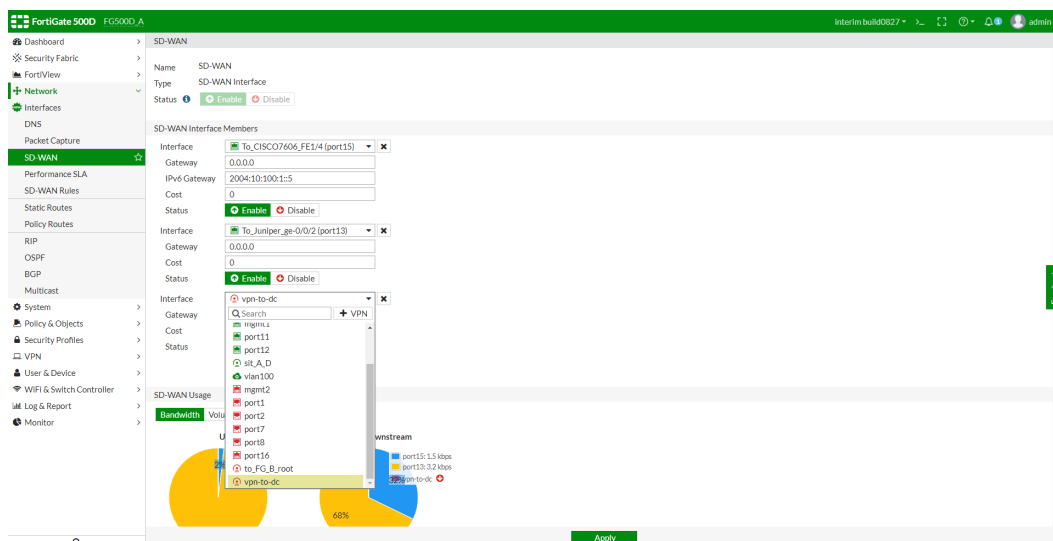
3. In the *Interface* drop-down, click **+VPN**. The *Create IPsec VPN for SD-WAN members* pane opens.



4. Enter the required information, then click *Create*.

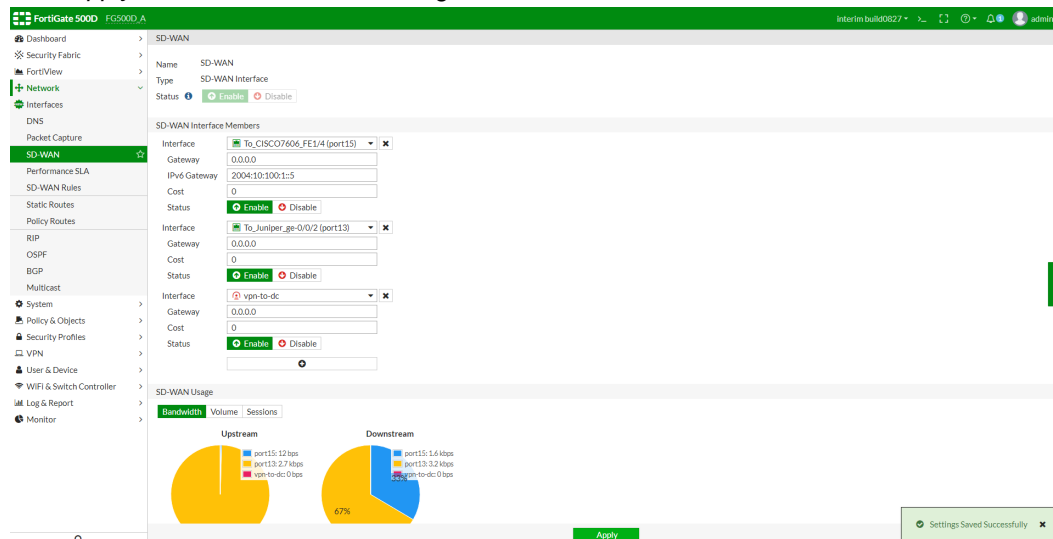


5. Click *Close* to return to the SD-WAN page.
The newly created VPN interface will be highlighted in the *Interface* drop-down list.



6. Select the VPN interface to add it as an SD-WAN member.

7. Click *Apply* to save the SD-WAN settings.

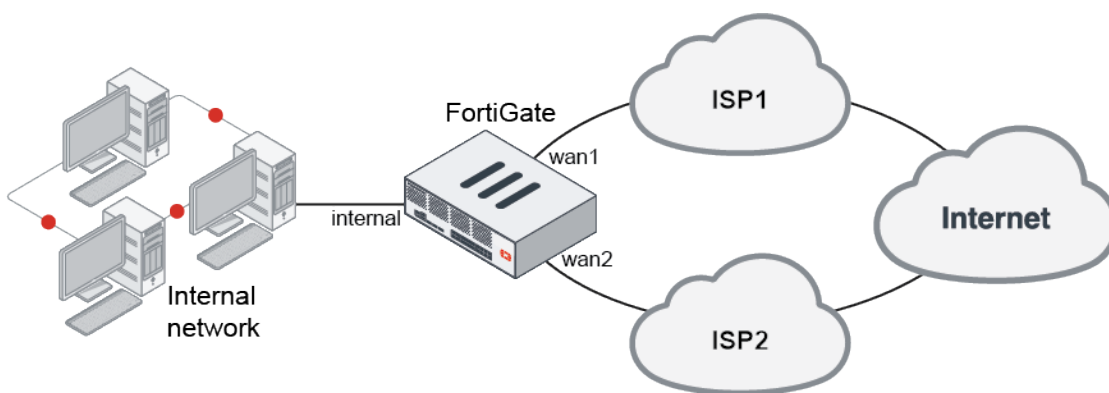


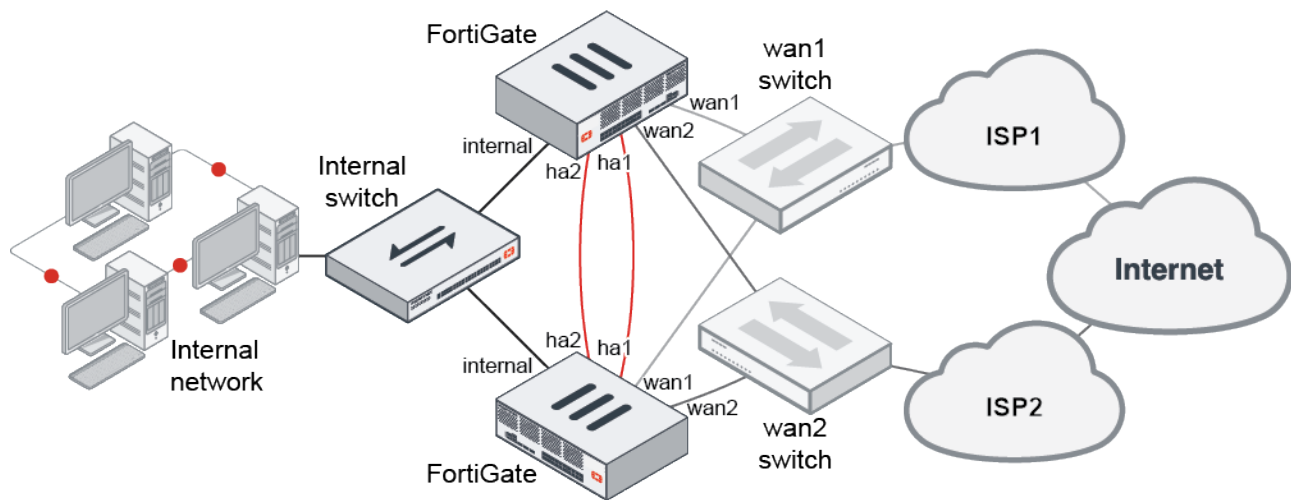
SD-WAN with FGCP HA

This example shows how to convert a standalone FortiGate SD-WAN solution to a FGCP HA cluster with full-mesh WAN set up. This configuration allows you to load balance your internet traffic between multiple ISP links. It also provides redundancy for your internet connection if your primary ISP is unavailable, or if one of the FortiGates in the HA cluster fails.

This example assumes that a standalone FortiGate has already been configured for SD-WAN by following the [SD-WAN quick start on page 451](#).

Standalone FortiGate:



FGCP HA cluster:

The following devices are required to convert the topology to HA:

- A second FortiGate that is the same model running the same firmware version.
- Two switches for connecting each FortiGate's WAN interface to the corresponding ISP modem.

Before you begin:

- Ensure that the licenses and subscriptions on both HA members match.
- Ensure that there are one or more ports reserved for HA heartbeat.
- Ensure you have physical access to both HA members.



Enabling HA and re-cabling the WAN interfaces will cause network interruptions.
This procedure should be performed during a maintenance window.

Configuring the standalone FortiGate for HA

After running the following commands, the FortiGate negotiates to establish an HA cluster. You might temporarily lose connectivity with the FortiGate as FGCP negotiations take place and the MAC addresses of the FortiGate interfaces are changed to HA virtual MAC addresses.

This configurations sets the HA mode to active-passive.

The ha1 and ha2 interfaces are configured as the heartbeat interfaces, with priorities set to 200 and 100 respectively. Setting different priorities for the heartbeat interfaces is a best practice, but is not required.

If you have more than one cluster on the same network, each cluster should have a different group ID. Changing the group ID changes the cluster interface's virtual MAC addresses. If the group IP causes a MAC address conflict on your network, select a different group ID.

Enabling override and increasing the device priority means that this FortiGate always becomes the primary unit.

To configure the standalone FortiGate for HA in the GUI:

1. Go to *System > Settings* and change the *Host name* so that the FortiGate can be easily identified as the primary unit.
2. Go to *System > HA* and configure the following options:

Mode	Active-Passive
Device priority	250
Group name	My-cluster
Password	<password>
Heartbeat interfaces	ha1 and ha2
Heartbeat Interface Priority	port2 (ha1): 200 port3 (ha2): 100



Override and the group ID can only be configured from the CLI.

3. Click **OK**.
Connectivity with the FortiGate will temporarily be lost.

To configure the standalone FortiGate for HA in the CLI:

1. Change the host name so that the FortiGate can be easily identified:

```
config system global
    set hostname primary_FG
end
```

2. Configure HA:

```
config system ha
    set mode a-p
    set group-id 100
    set group-name My-cluster
```

```

set password <password>
set priority 250
set override enable
set hbdev ha1 200 ha2 100
end

```



If HA mode does not start after running the above steps, ensure that none of the FortiGate's interfaces use DHCP or PPPoE addressing.

Configuring the secondary FortiGate for HA

The secondary FortiGate must be the same model and running the same firmware version as the primary FortiGate. The HA settings are the same as the for the primary unit, except the secondary device has a lower priority and override is not enabled.



It is best practice to reset the FortiGate to factory default settings prior to configuring HA. This reduces the chance of synchronization problems.

```

# execute factoryreset
This operation will reset the system to factory default!
Do you want to continue? (y/n) y

```

This is unnecessary if the device is new from the factory.

To configure the secondary FortiGate for HA in the GUI:

1. Go to *System > Settings* and change the *Host name* so that the FortiGate can be easily identified as the backup unit.
2. Go to *System > HA* and configure the options the same as for the primary FortiGate, except with a lower priority:

Mode	Active-Passive
Device priority	128
Group name	My-cluster
Password	<password>
Heartbeat interfaces	ha1 and ha2
Heartbeat Interface Priority	port2 (ha1): 200 port3 (ha2): 100

3. Click *OK*.

To configure the secondary FortiGate for HA in the CLI:

1. Change the host name so that the secondary FortiGate can be easily identified:

```

config system global
    set hostname secondary_FG
end

```

2. Configure HA:

```
config system ha
    set mode a-p
    set group-id 100
    set group-name My-cluster
    set password <password>
    set priority 128
    set hbdev ha1 200 ha2 100
end
```

Connecting the heartbeat interfaces between the FortiGates

To connect and check the heartbeat interfaces:

1. Connect the heartbeat interfaces ha1 and ha2 between the primary and secondary FortiGate.
 - a. An HA primary is selected. Because the primary FortiGate has a higher priority and override enabled, it assumes the role of HA primary.
 - b. The secondary FortiGate synchronizes its configuration from the primary device.
2. Verify that the checksums match between the primary and secondary FortiGates:

```
# diagnose sys ha checksum cluster
```

If all of the cluster members have identical checksums, then their configurations are synchronized. If the checksums are not the same, wait for a few minutes, then repeat the command. Some parts of the configuration might take a significant amount of time to synchronize (tens of minutes).

Connecting other traffic interfaces

After the device configurations are synchronized, you can connect the rest of the traffic interfaces. Making these connections will disrupt traffic as cables are disconnected and reconnected.

Switches must be used between the cluster and the ISPs, and between the cluster and the internal network, as shown in the topology diagram.

Checking cluster operations

The *HA Status* dashboard widget shows the synchronization status. Hover over the host names of each FortiGate in the widget to verify that they are synchronized and have the same checksum.







To view more information about the cluster status, including the number of sessions passing through the cluster members, go to *System > HA*.

See [Check HA sync status on page 688](#) for more information.

Results

1. Browse the internet on a computer in the internal network.
2. Go to *Network > SD-WAN* to see the bandwidth, volume, and sessions for traffic on the SD-WAN interfaces. See [Results on page 457](#) for details.

3. Go to *Monitor > SD-WAN Monitor* to see information about each interface, such as the number of sessions and the bit rate.

+	Interface	Status	Sessions	Upload	Download
	sd-wan				
→	wan1		68 	255 B/s 	4.03 kB/s 
→	wan2		30 	174 B/s 	715 B/s 

Testing HA failover

All traffic should currently be flowing through the primary FortiGate. If it becomes unavailable, traffic fails over to the secondary FortiGate. When the primary FortiGate rejoins the cluster, the secondary FortiGate continues to operate as the primary FortiGate.

To test this, ping a reliable IP address from a computer in the internal network, and then power off the primary FortiGate.

There will be a momentary pause in the ping results until traffic diverts to the backup FortiGate, allowing the ping traffic to continue:

```
64 bytes from 184.25.76.114: icmp_seq=69 ttl=52 time=8.719 ms\
64 bytes from 184.25.76.114: icmp_seq=70 ttl=52 time=8.822 ms\
64 bytes from 184.25.76.114: icmp_seq=74 ttl=52 time=8.901 ms\
Request timeout for icmp_seq 75\
64 bytes from 184.25.76.114: icmp_seq=76 ttl=52 time=8.860 ms\
64 bytes from 184.25.76.114: icmp_seq=77 ttl=52 time=9.174 ms\
64 bytes from 184.25.76.114: icmp_seq=83 ttl=52 time=8.639 ms}
```



If you are using port monitoring, you can also unplug the primary FortiGate's internet facing interface to test failover.







After the secondary FortiGate becomes the primary, you can log into the cluster using the same IP address as before the fail over. If the primary FortiGate is powered off, you will be logged into the backup FortiGate. Check the host name to verify what device you have logged into. The FortiGate continues to operate in HA mode, and if you restart the primary FortiGate, it will rejoin the cluster and act as the backup FortiGate. Traffic is not disrupted when the restarted FortiGate rejoins the cluster.

Testing ISP failover

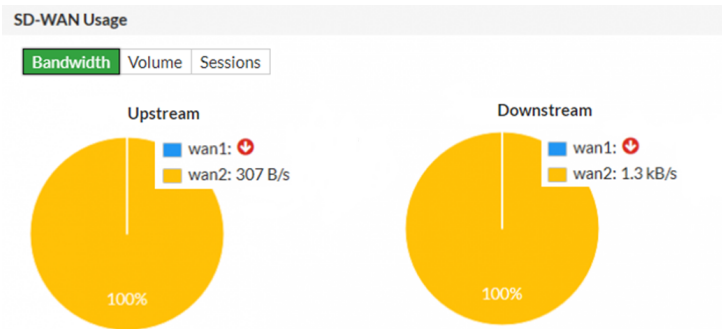
To test a failover of the redundant internet configuration, you need to simulate a failed internet connection to one of the ports. You can do this by disconnecting power from the wan1 switch, or by disconnecting the wan1 interfaces of both FortiGates from ISP1.

After disconnecting, verify that users still have internet access

- Go to *Dashboard > Network*, and expand the *SD-WAN* widget. The *Upload* and *Download* columns for wan1 show that traffic is not going through that interface.

+	Interface	Status	Sessions	Upload	Download
	sd-wan				
→	wan1		16 	0 B/s 	0 B/s 
→	wan2		103 	242 B/s 	1.24 kB/s 

- Go to *Network > SD-WAN*. The *Bandwidth*, *Volume*, and *Sessions* tabs show that traffic is entirely diverted to wan2.



Users on the network should not notice the wan1 failure. If you are using the wan1 gateway IP address to connect to the administrator dashboard, it will appear as though you are still connecting through wan1.

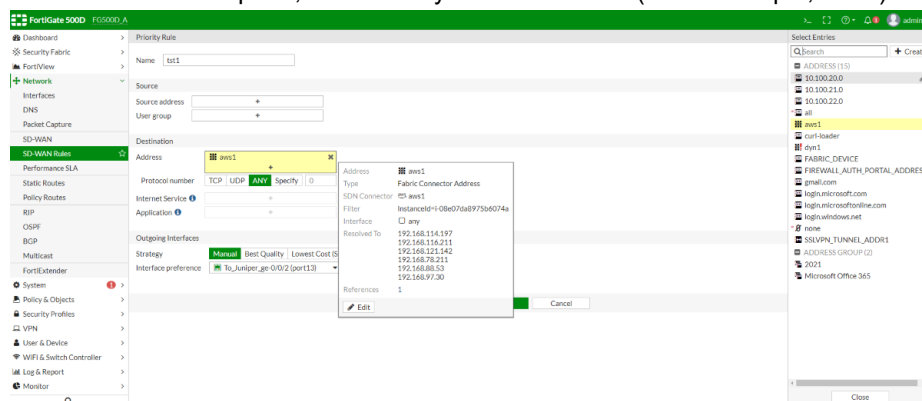
After verifying a successful failover, reestablish the connection to ISP1.

Enable dynamic connector addresses in SD-WAN policies

Dynamic Fabric Connector addresses can be used in SD-WAN policies.

To add a dynamic connector address to an SD-WAN rule:

- Go to *Network > SD-WAN Rules*.
- Click *Create New*.
- In the *Name* field, enter the rule name.
- In the *Destination > Addresses* field, click the +. The *Select Entries* pane will appear.
- In the *Select Entries* pane, select the dynamic connector (in the example, *aws1*).



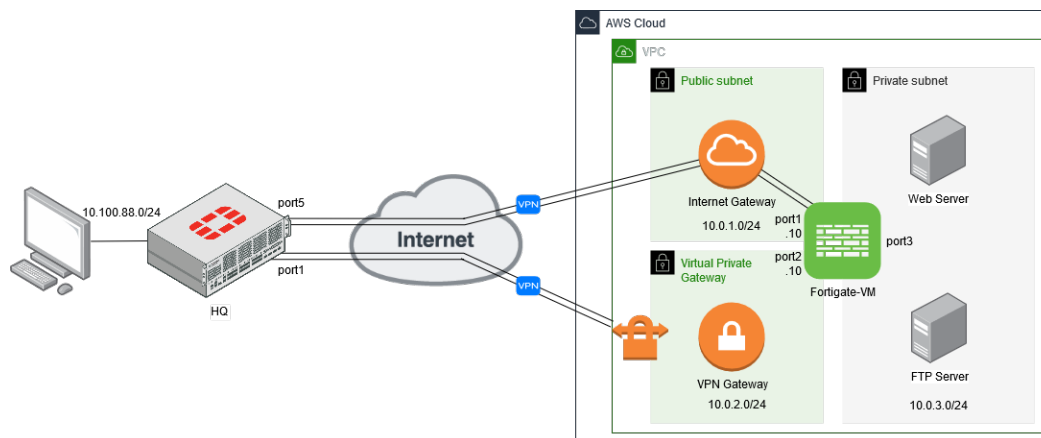
- Configure the remaining settings as required.
- Click *OK* to save the rule.

SD-WAN cloud on-ramp

In this example, you configure a connection to a new cloud deployment that has some remote servers. SD-WAN is used to steer traffic through the required overlay tunnel.

The on-premise FortiGate has two internet connections, each with a single VPN connection. The two VPN gateways are configured on the cloud for redundancy, one terminating at the FortiGate-VM, and the other at the native AWS VPN Gateway.

This example uses AWS as the Infrastructure as a Service (IaaS) provider, but the same configuration can also apply to other services. A full mesh VPN setup is not shown, but can be added later if required.



To connect to the servers that are behind the cloud FortiGate-VM, virtual IP addresses (VIPs) are configured on port2 to map to the servers:

- VPN traffic terminating on port1 is routed to the VIP on port2 to access the web servers.
- VPN traffic terminating on the VPN gateway accesses the VIPs on port2 directly.

There are four major steps to configure this setup:

1. [Configuring the VPN overlay between the HQ FortiGate and cloud FortiGate-VM on page 562](#)
2. [Configuring the VPN overlay between the HQ FortiGate and AWS native VPN gateway on page 567](#)
3. [Configuring the VIP to access the remote servers on page 571](#)
4. [Configuring the SD-WAN to steer traffic between the overlays on page 573](#)

After the configuration is complete, verify the traffic to ensure that the configuration is working as expected, see [Verifying the traffic on page 577](#).

Configuring the VPN overlay between the HQ FortiGate and cloud FortiGate-VM

Configure the cloud FortiGate-VM

To create an address for the VPN gateway:

1. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
2. Set Name to *local_subnet_10_0_2_0*.

3. Set *IP/Netmask* to *10.0.2.0/24*.

New Address

Name: local_subnet_10_0_2_0

Color: Change

Type: Subnet

IP/Netmask: 10.0.2.0/24

Interface: any

Show in address list: ☒

Static route configuration: ☐

Comments: Write a comment... 0/255

Dynamic Address

Guides

- Configuring an AWS Dynamic Address
- Configuring an Azure Dynamic Address
- Configuring a Google Cloud Platform Dynamic Address
- Configuring an Oracle Cloud Infrastructure Dynamic Address
- Configuring an OpenStack Dynamic Address

Documentation

- Online Help
- Video Tutorials

OK Cancel

4. Click *OK*.

To configure a custom IPsec VPN:

- Go to *VPN > IPsec Wizard*.
- Set *Name* to *Core_Dialup*.
- Set *Template type* to *Custom*.

VPN Creation Wizard

VPN Setup

Name: Core_Dialup

Template type: Site to Site Hub-and-Spoke Remote Access Custom

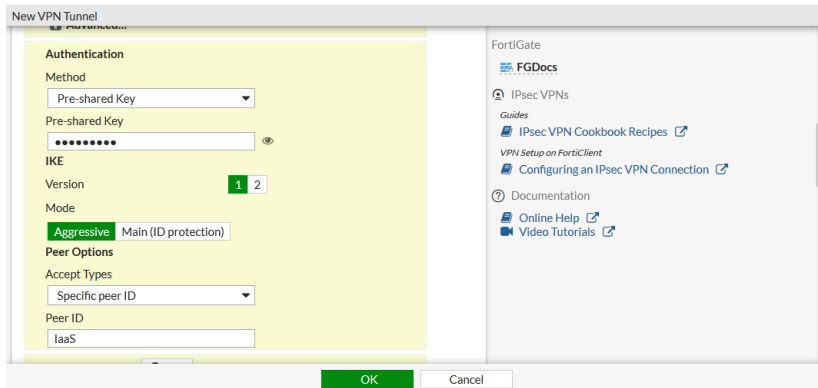
< Back Next > Cancel

- Click *Next*.
- Configure *Network* settings:

Remote Gateway	Dialup User
Interface	port1
NAT Traversal	Enable

6. Configure *Authentication* settings:

Method	Pre-shared Key
Pre-shared Key	Enter the pre-shared key.
Version	1
Mode	Aggressive This setting allows the peer ID to be specified.
Accept Types	Specific peer ID
Peer ID	laaS The other end of the tunnel needs to have its local ID set to laaS.



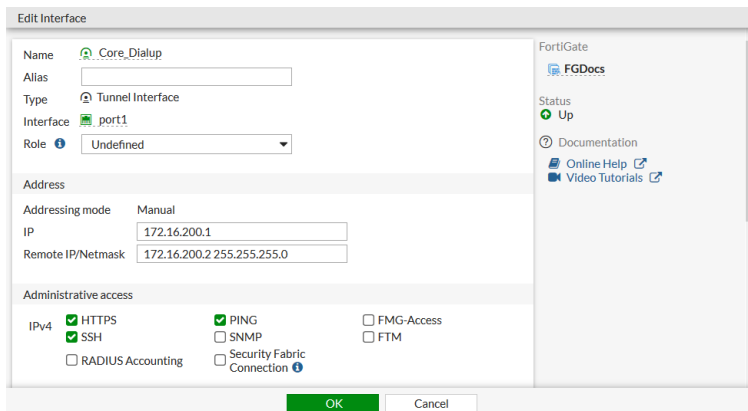
7. Leave the default *Phase 1 Proposal* settings and disable *XAUTH*.
8. Configure the *Phase 2 Selector* settings:

Name	Ent_Core
Local Address	Named Address - <i>local_subnet_10_0_2_0</i>
Remote Address	Named Address - <i>all</i> This setting allows traffic originating from both the remote subnet 10.100.88.0 and the health checks from the VPN interface on the remote FortiGate. For increased security, each subnet can be specified individually.

9. Click **OK**.

To configure remote and local tunnel IP addresses:

1. Go to *Network > Interfaces* and edit the *Core_Dialup* interface under *port1*.
2. Set *IP* to 172.16.200.1.
3. Set *Remote IP/Netmask* to 172.16.200.2 255.255.255.0. This is where remote health check traffic will come from.
4. Enable *Administrative access* for *HTTPS*, *PING*, and *SSH*.



5. Click **OK**.

To configure a route to the remote subnet through the tunnel:

1. Go to *Network > Static Routes* and click *Create New*.
2. Set *Destination* to *Subnet* and enter the IP address and netmask: 10.100.88.0/255.255.255.0.

3. Set *Interface* to *Core_Dialup*.

4. Click *OK*.

To configure a firewall policy to allow traffic from the tunnel to port2:

1. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
2. Configure the following:

Name	Core_Dialup-to-port2
Incoming Interface	Core_Dialup
Outgoing Interface	port2
Source	all
Destination	local_subnet_10_0_2_0
Schedule	always
Service	ALL
Action	ACCEPT

3. Configure the remaining settings as required.
4. Click *OK*.

Configure the HQ FortiGate

To create an address for the VPN gateway:

1. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
2. Set *Name* to *remote_subnet_10_0_2_0*.

3. Set *IP/Netmask* to *10.0.2.0/24*.
4. Click *OK*.

To configure a custom IPsec VPN:

1. Go to *VPN > IPsec Wizard*.
2. Set *Name* to *FGT_AWS_Tun*.
3. Set *Template type* to *Custom*.
4. Click *Next*.
5. Configure *Network* settings:

Remote Gateway	Static IP Address
IP Address	100.21.29.17
Interface	port5
NAT Traversal	Enable

6. Configure *Authentication* settings:

Method	Pre-shared Key
Pre-shared Key	Enter the pre-shared key.
Version	1
Mode	Aggressive This setting allows the peer ID to be specified.
Accept Types	Any peer ID

7. Leave the default *Phase 1 Proposal* settings, except set *Local ID* to *laaS*.
8. Disable *XAUTH*.
9. Configure the *Phase 2 Selector* settings:

Name	FGT_AWS_Tun
Local Address	Named Address - <i>all</i> This setting allows traffic originating from both the local subnet 10.100.88.0 and the health checks from the VPN interface. For increased security, each subnet can be specified individually.
Remote Address	Named Address - <i>remote_subnet_10_0_2_0</i>

10. Click *OK*.

To configure local and remote tunnel IP addresses:

1. Go to *Network > Interfaces* and edit the *FGT_AWS_Tun* interface under *port5*.
2. Set *IP* to *172.16.200.2*.
3. Set *Remote IP/Netmask* to *172.16.200.1 255.255.255.0*.
4. Enable *Administrative access* for *HTTPS*, *PING*, and *SSH*.
5. Click *OK*.



Routing is defined when creating the SD-WAN interface. The firewall policy is created after the SD-WAN interface is defined.

Configuring the VPN overlay between the HQ FortiGate and AWS native VPN gateway

This example uses static routing. It is assumed that the AWS VPN Gateway is already configured, and that proper routing is applied on the corresponding subnet.

Verify the AWS configuration

See [Creating routing tables and associate subnets](#) in the [AWS Administration Guide](#) for configuration details.

To check the AWS configuration:

1. Go to *Virtual Private Network (VPN) > Customer Gateways* to confirm that the customer gateway defines the FortiGate IP address as its Gateway IP address, in this case **34.66.121.231**.

Name	ID	State	Type	IP Address	BGP ASN	VPC
cloud-onramp-dome	vpc-0578d871da32a68	available	ipsec.1	34.66.121.231	65000	vpc-0731da0288fa30352 Cloud_onRamp

2. Go to *Virtual Private Network (VPN) > Virtual Private Gateways* to confirm that a virtual private gateway (VPG) has been created. In this case it is attached to the *Cloud_onRamp* VPC that contains the FortiGate and servers.

Name	ID	State	Type	VPC	ASN (Amazon side)
Cloud_onRamp_VPG	vpc-0473a045b75a5a2	attached	ipsec.1	vpc-0731da0288fa30352 Cloud_onRamp	64512

3. Go to *Virtual Private Network (VPN) > Site-to-Site VPN Connections* to confirm that site-to-site VPN connections have been created and attached to the customer gateway and virtual private gateway.

If *Routing Options* is *Static*, the IP prefix of the remote subnet on the HQ FortiGate (10.100.88.0) is entered here.

Name	VPN ID	State	Virtual Private Gateway	Transit Gateway	Customer Gateway	Customer Gateway Address
Cloud_onRamp_VPN	vpc-0473a045b75a5a2	available	vpc-0473a045b75a5a2 Cloud...	-	vpc-0578d871da32a68 cloud-onramp-dome	34.66.121.231

VPN Connection: vpc-0473a045b75a5a2			
Details	Tunnel Details	Static Routes	Tags
VPN ID	vpc-0473a045b75a5a2	State	available
Virtual Private Gateway	vpc-0473a045b75a5a2 Cloud_onRamp_VPG	Customer Gateway	vpc-0578d871da32a68 cloud-onramp-dome
Transit Gateway	-	Customer Gateway Address	34.66.121.231
Type	ipsec.1	Category	VPN
VPC	vpc-0731da0288fa30352 Cloud_onRamp	Routing	Static
Acceleration Enabled	false	Authentication Type	Pre-Shared Key

AWS site-to-site VPN always creates two VPN tunnels for redundancy. In this example, only Tunnel 1 is used.

Create VPN Connection Download Configuration Actions

Filter by tags and attributes or search by keyword

Name	VPN ID	State	Virtual Private Gateway	Transit Gateway	Custom
Cloud_onRamp_VPN	vpn-04f1b6daf1ea91694	available	vgw-04f3e045b75aea6a2 Clou...	-	cgw-057

VPN Connection: vpn-04f1b6daf1ea91694

Details Tunnel Details Static Routes Tags

Tunnel State

Tunnel Number	Outside IP Address	Inside IP CIDR	Status	Status Last Changed	D
Tunnel 1	34.210.19.225	169.254.55.152/30	UP	June 1, 2020 at 7:47:13 PM UTC-7	-
Tunnel 2	52.36.216.244	169.254.170.32/30	DOWN	May 27, 2020 at 6:48:47 PM UTC-7	-

- Click *Download Configuration* to download the FortiGate's tunnel configurations. The configuration can be referred to when configuring the FortiGate VPN.
- The new VPG is attached to your VPC, but to successfully route traffic to the VPG, proper routing must be defined. Go to *Virtual Private Cloud > Subnets*, select the *Cloud-OnRamp-VPN*, and select the *Route Table* tab to verify that there are at least two routes to send traffic over the VPG.

New VPC Experience Tell us what you think

VPC Dashboard

Filter by VPC: Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways New

Egress Only Internet Gateways

DHCP Options Sets New

Elastic IPs New

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

SECURITY

Network ACLs

Security Groups New

Create subnet Actions

search: OnRamp Add filter

Name	Subnet ID	State
Cloud-OnRamp-VPN	subnet-05274b366e1f86f6e	available
COR-Public subnet	subnet-06afbec06f9e77116	available
Cloud-OnRamp-WAN	subnet-0710596c18f5e8332	available
Cloud-OnRamp-Server	subnet-0a77de9bc8336a223	available
COR-Private subnet	subnet-0e92905e2d422503a	available

Subnet: subnet-05274b366e1f86f6e

Description Flow Logs Route Table Network ACL Tags

Edit route table association

Route Table: rtb-07808d343673d657c | Cloud-OnRamp-VPN-Routetable

Destination	Target
169.254.0.0/16	vgw-04f3e045b75aea6a2
10.0.0.0/16	local
10.100.0.0/16	vgw-04f3e045b75aea6a2

- 169.254.0.0/24 defines the tunnel IP address. Health check traffic originating from the FortiGate will come from this IP range.
 - 10.100.0.0/16 defines the remote subnet from the HQ FortiGate.
 - Both routes point to the just created VPG *vgw-04xxxx*.
- On the cloud FortiGate-VM EC2 instances, ensure that port1 and port2 both have *Source/Dest. Check* set to *false*. This allows the FortiGate to accept and route traffic to and from a different network. If you launched the instance from the AWS marketplace, this setting defaults to *true*.

Network Interface eth0	
Interface ID	eni-00e636a0812a17130
VPC ID	vpc-0731da92869a30352
Attachment Owner	585196279398
Attachment Status	attached
Attachment Time	Wed May 27 18:38:55 GMT-700 2020
Delete on Terminate	true
Private IP Address	10.0.1.10
Private DNS Name	-
Public IP Address	1.1.1.1
Source/Dest. Check	false
Description	Primary network interface
Security Groups	Fortinet FortiGate Next-Generation Firewall-v6-4-0-AutogenByAWSMP-
Elastic Fabric Adapter	Disabled

Configure routing to the VPG on the cloud FortiGate-VM

To configure routing to the VPG on the cloud FortiGate-VM:

1. Go to *Network > Static Routes* and click *Create New*.
2. Set *Destination* to *Subnet* and enter the IP address and netmask: *10.100.88.0/255.255.255.0*.
3. Set *Gateway Address* to *Specify* and enter *10.0.2.1*.
4. Set *Interface* to *port2*.

New Static Route

Dynamic Gateway ☐

Destination

10.100.88.0/255.255.255.0

Gateway Address

Interface

Administrative Distance

Comments 0/255

Status ☒ Enabled ☐ Disabled

Advanced Options

The new route must have the same *Administrative Distance* as the route that was created for traffic through the *Core_Dialup* tunnel to ensure that both routes are added to the routing table (see [To configure a route to the remote subnet through the tunnel](#)).

The *Gateway Address* is arbitrarily set to 10.0.2.1. The VPG does not have an IP address, but the address defined here allows the FortiGate to route traffic out of port2, while AWS routes the traffic based on its routing table.

5. Click *OK*.
6. Go to *Network > Static Routes* to view the configured static routes:

Destination	Gateway IP	Interface	Status	Comments
10.100.88.0/24		Core_Dialup	Enabled	
10.100.88.0/24	10.0.2.1	port2	Enabled	

7. Go to *Monitor > Routing Monitor* to view the routing table.

Type	Network	Gateway IP	Interfaces	Distance
Static	0.0.0.0/0	10.0.1.1	port1	5
Static	0.0.0.0/0	10.0.2.1	port2	5
Connected	10.0.1.0/24	0.0.0.0	port1	0
Connected	10.0.2.0/24	0.0.0.0	port2	0
Connected	10.0.3.0/24	0.0.0.0	port3	0
Static	10.100.88.0/24	0.0.0.0	Core_Dialup	10
Static	10.100.88.0/24	10.0.2.1	port2	10
Connected	172.16.200.0/24	0.0.0.0	Core_Dialup	0
Connected	172.16.200.1/32	0.0.0.0	Core_Dialup	0

Configure IPsec VPN on the HQ FortiGate

To configure a custom IPsec VPN:

1. Go to *VPN > IPsec Wizard*.
2. Set *Name* to *AWS_VPG*.
3. Set *Template type* to *Custom*.
4. Click *Next*.
5. Configure *Network* settings:

Remote Gateway	Static IP Address
IP Address	34.210.19.225 This address is taken from the downloaded AWS configuration file.
Interface	port1
NAT Traversal	Enable

6. Configure *Authentication* settings:

Method	Pre-shared Key
Pre-shared Key	Enter the pre-shared key.
Version	1
Mode	Main

7. Configure the *Phase 1 Proposal* settings using information from the downloaded AWS configuration file.
8. Disable *XAUTH*.
9. Configure the *Phase 2 Selector* settings:

Name	AWS_VPG
Local Address	Named Address - <i>all</i> This setting allows traffic originating from both the local subnet 10.100.88.0 and the health checks from the VPN interface. For increased security, each subnet can be specified individually.
Remote Address	Named Address - <i>remote_subnet_10_0_2_0</i>

10. Click *OK*.

To configure local and remote tunnel IP addresses:

1. Go to *Network > Interfaces* and edit the *AWS_VPG* interface under *port1*.
2. Set *IP* to *169.254.55.154*.
3. Set *Remote IP/Netmask* to *169.254.55.153 255.255.255.0*.
4. Enable *Administrative access* for *HTTPS* and *PING*.
5. Click *OK*.



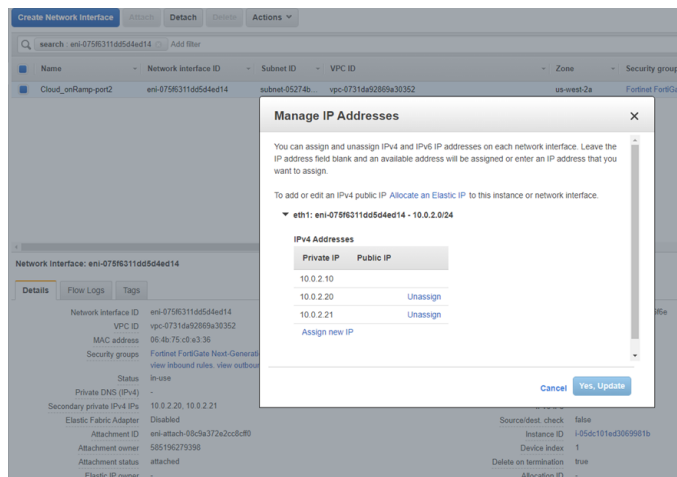
Routing is defined when creating the SD-WAN interface. The firewall policy is created after the SD-WAN interface is defined.

Configuring the VIP to access the remote servers

VIPs, interface IP addresses, and policies are created on the cloud FortiGate-VM to allow access to the remote servers.

To configure additional private IPs on AWS for the FortiGate VIP:

1. On the FortiGate EC2 instance, edit the *Elastic Network Interface* that corresponds to *port2*. In this example, Network Interface *eth1*.
2. Go to *Actions > Manage IP Addresses*.
3. Add two private IP address in the 10.0.2.0/24 subnet.
These address will be used in the VIPs on the FortiGate. This ensures that traffic to these IP addresses is routed to the FortiGate by AWS.



4. Click *Yes, Update*.

To configure VIPs on the cloud FortiGate-VM:

1. Go to *Policy & Objects > Virtual IPs* and click *Create New > Virtual IP*.
2. Configure the following:

Name	VIP-HTTP
Interface	port2
External IP address/range	10.0.2.20
Mapped IP address/range	10.0.3.33

3. Click **OK**.
4. Create a second VIP for the FTP server with the following settings:

Name	VIP-FTP
Interface	port2
External IP address/range	10.0.2.21
Mapped IP address/range	10.0.3.44

+ Create New Edit Clone Delete <input type="text" value="Search"/>				
Name	Details	Interfaces	Services	Ref
IPv4 Virtual IP				
VIP-HTTP	10.0.2.20 → 10.0.3.33	port2		0
VIP-FTP	10.0.2.21 → 10.0.3.44	port2		0

To configure firewall policies to allow traffic from port2 to port3:

1. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
2. Configure the following:

Name	To-WebServer
Incoming Interface	port2
Outgoing Interface	port3
Source	all
Destination	VIP-HTTP
Schedule	always
Service	ALL
Action	ACCEPT
NAT	Enabled

3. Configure the remaining settings as required.
4. Click **OK**.
5. Create a second policy for the FTP VIP with the following settings:

Name	To-FTP
Incoming Interface	port2
Outgoing Interface	port3
Source	all
Destination	VIP-FTP
Schedule	always
Service	ALL
Action	ACCEPT
NAT	Enabled

6. Click **OK**.

<div>+ Create New</div>		<div>Edit</div>	<div>Delete</div>	<div>Policy Lookup</div>	<div>Search</div>			<div>Q</div>	<div>Interface Pair View</div>		<div>By Sequence</div>
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes		
<div><div></div> <div>Core_Dialup → port2</div> <div>1</div></div>											
Core_Dialup-to-port2	<div>all</div>	<div>local_subnet_10_0_2_0</div>	<div>always</div>	<div>ALL</div>	<div>✓ ACCEPT</div>	<div>✓ Enabled</div>	<div>SSL no-inspection</div>	<div>UTM</div>	6.49 MB	<div></div>	
<div><div></div> <div>port2 → port3</div> <div>2</div></div>											
To-WebServer	<div>all</div>	<div>VIP-HTTP</div>	<div>always</div>	<div>ALL</div>	<div>✓ ACCEPT</div>	<div>✓ Enabled</div>	<div>SSL no-inspection</div>	<div>UTM</div>	20.12 kB	<div></div>	
To-FTP	<div>all</div>	<div>VIP-FTP</div>	<div>always</div>	<div>ALL</div>	<div>✓ ACCEPT</div>	<div>✓ Enabled</div>	<div>SSL no-inspection</div>	<div>UTM</div>	10.11 kB	<div></div>	
<div><div></div> <div>Implicit</div> <div>1</div></div>											

Configuring the SD-WAN to steer traffic between the overlays

Configure the HQ FortiGate to use two overlay tunnels for SD-WAN, steering HTTPS and HTTP traffic through the FGT_AWS_Tun tunnel, and SSH and FTP through the AWS_VPG tunnel.

1. [Add SD-WAN member interfaces](#)
2. [Configure a route to the remote network](#)
3. [Configure firewall policies](#)

4. [Configure a health check](#)
5. [Configure SD-WAN rules](#)

To add SD-WAN member interfaces:

1. Go to *Network > SD-WAN*
2. Set *Status* to *Enable*.
3. In the *SD-WAN Interface Members* table, click *Create New*.
4. Set *Interface* to *AWS_VPG* then click *OK*.

SD-WAN New SD-WAN Member

Name: SD-WAN

Type: SD-WAN Interface

Status: Enable Disable

Interface: AWS_VPG

Gateway: 0.0.0.0

Cost: 0

OK Cancel

5. Click *Create New* again.
6. Set *Interface* to *FGT_AWS_Tun*.
7. Set *Gateway* to *172.16.200.1*.
8. Click *OK*.

SD-WAN

Name: SD-WAN

Type: SD-WAN Interface

Status: Enable Disable

SD-WAN Interface Members

Create New Edit Delete

Interfaces	Gateway	Cost
AWS_VPG	0.0.0.0	0
FGT_AWS_Tun	172.16.200.1	0

SD-WAN Usage

Bandwidth Volume Sessions

Upstream

Downstream

Apply

To configure a route to the remote network 10.0.2.0/24:

1. Go to *Network > Static Routes* and click *Create New*.
2. Set *Destination* to *Subnet* and enter the IP address and netmask: *10.0.2.0/255.255.255.0*.
3. Set *Interface* to *SD-WAN*.

New Static Route

Dynamic Gateway: Dynamic

Destination: Subnet Internet Service

10.0.2.0/255.255.255.0

Interface: SD-WAN

Comments: Write a comment...

Status: Enabled Disabled

OK Cancel

4. Click **OK**.

To configure firewall policies to allow traffic from the internal subnet to SD-WAN:

1. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
2. Configure the following:

Name	ISFW-to-laaS
Incoming Interface	port3
Outgoing Interface	SD-WAN
Source	all
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT
NAT	Enabled

3. Configure the remaining settings as required.
4. Click **OK**.
Once the firewall policies are configured, the VPN tunnels should come up when there is traffic.

To configure a health check to monitor the status of the tunnels:

As you are accessing the servers on the 10.0.2.0/24 subnet, it is preferable to use the FortiGate port2 interface as the ping server for detection. This ensures that, if the gateway is not reachable in either tunnel, its routes are brought down and traffic continues on the other tunnel.

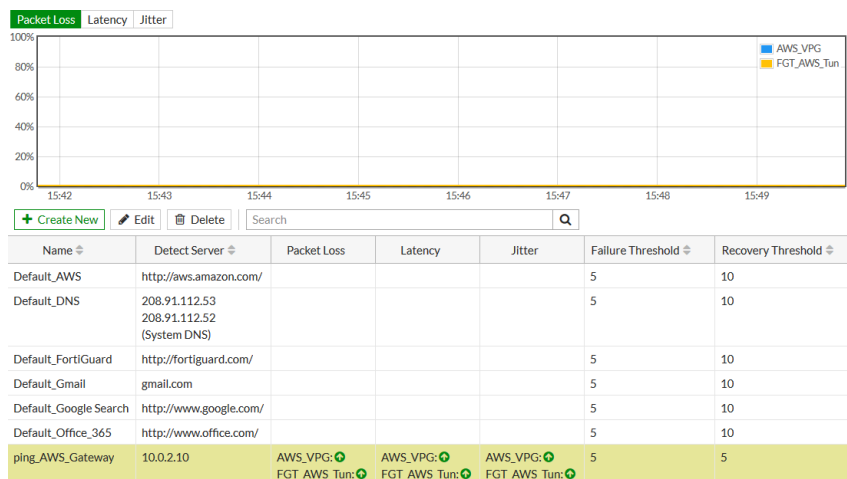
1. Go to *Network > Performance SLA* and click *Create New*.
2. Configure the following:

Name	ping_AWS_Gateway
Protocol	Ping

Server 10.0.2.10

Participants Add AWS_VPG and FGT_AWS_Tun as participants.

3. Click OK.



Health check probes originate from the VPN interface's IP address. This is why the phase2 selectors are configured with *Local Address* set to *all*.

To configure SD-WAN rules to steer traffic:

HTTPS and HTTP traffic is steered to the FGT_AWS_Tun tunnel, and SSH and FTP traffic is steered to the AWS_VPG tunnel. The Manual algorithm is used in this example.

1. Go to *Network > SD-WAN Rules* and click *Create New*.
2. Configure the following:

Name	http-to-FGT_AWS_Tun
Source Address	all
Address	remote_subnet_10_0_2_0

Protocol	TCP
Port range	80 - 80
Outgoing Interfaces	Manual
Interface preference	FGT_AWS_Tun

Priority Rule

Name:

Source

Source address:

User group:

Destination

Address:

Protocol number:

Port range: -

Internet Service:

Application:

Outgoing Interfaces

Strategy:

Interface preference:

Status:

OK Cancel

SD-WAN Rules Setup Guides

- [Implicit Rule](#)
- [Best Quality](#)
- [Lowest Cost \(SLA\)](#)
- [Maximize Bandwidth \(SLA\)](#)

Documentation

- [Online Help](#)
- [Video Tutorials](#)

3. Click **OK**.

4. Create other SD-WAN rules as required:

[+ Create New](#) [Edit](#) [Delete](#)

ID	Name	Source	Destination	Criteria	Members
IPv4					
1	http-to-FGT_AWS_Tun	all	remote_subnet_10_0_2_0		FGT_AWS_Tun
2	ssh-to-AWS_VPG	all	remote_subnet_10_0_2_0		AWS_VPG
3	https-to-FGT_AWS_Tun	all	remote_subnet_10_0_2_0		FGT_AWS_Tun
4	ftp-to-AWS_VPG	all	FTP-Server		AWS_VPG
Implicit					
	sd-wan	all	all	Source IP	any

Verifying the traffic

To verify that pings are sent across the IPsec VPN tunnels

- On the HQ FortiGate, run the following CLI command:

```
# diagnose sniffer packet any 'host 10.0.2.10' 4 0 1 interfaces=[any]
filters=[host 10.0.2.10]
2020-06-05 11:35:14.822600 AWS_VPG out 169.254.55.154 -> 10.0.2.10: icmp: echo request
2020-06-05 11:35:14.822789 FGT_AWS_Tun out 172.16.200.2 -> 10.0.2.10: icmp: echo request
2020-06-05 11:35:14.877862 FGT_AWS_Tun in 10.0.2.10 -> 172.16.200.2: icmp: echo reply
2020-06-05 11:35:14.878887 AWS_VPG in 10.0.2.10 -> 169.254.55.154: icmp: echo reply
```

- On the cloud FortiGate-VM, run the following CLI command:

```
# diagnose sniffer packet any 'host 10.0.2.10' 4 0 1 interfaces=[any]
filters=[host 10.0.2.10]
2020-06-05 11:37:57.176329 port2 in 169.254.55.154 -> 10.0.2.10: icmp: echo request
```

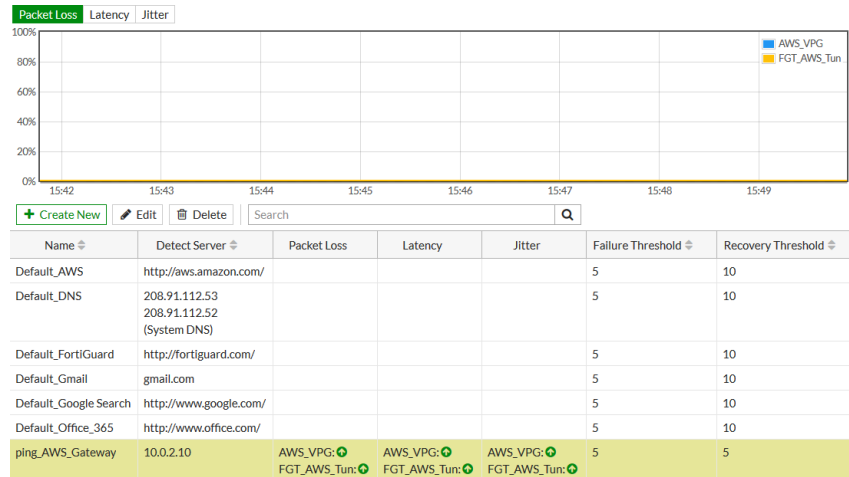
```

2020-06-05 11:37:57.176363 port2 out 10.0.2.10 -> 169.254.55.154: icmp: echo reply
2020-06-05 11:37:57.176505 Core_Dialup in 172.16.200.2 -> 10.0.2.10: icmp: echo request
2020-06-05 11:37:57.176514 Core_Dialup out 10.0.2.10 -> 172.16.200.2: icmp: echo reply

```

To verify the SLA health checks on the HQ FortiGate:

1. Go to **Network > Performance SLA** and select **Packet Loss** and the **ping_AWS_Gateway** SLA:



2. Run the following CLI command:

```

# diagnose sys sdwan health-check
...
Seq(1 AWS_VPG): state(alive), packet-loss(0.000%) latency(56.221), jitter(0.290) sla_map=0x0
Seq(2 FGT_AWS_Tun): state(alive), packet-loss(0.000%) latency(55.039), jitter(0.223)
sla_map=0x0

```

To verify service rules:

1. Go to **Network > SD-WAN Rules**:

ID	Name	Source	Destination	Criteria	Members
1	http-to-FGT_AWS_Tun	all	remote_subnet_10_0_2_0		FGT_AWS_Tun
2	ssh-to-AWS_VPG	all	remote_subnet_10_0_2_0		AWS_VPG
3	https-to-FGT_AWS_Tun	all	remote_subnet_10_0_2_0		FGT_AWS_Tun
4	ftp-to-AWS_VPG	all	FTP-Server		AWS_VPG
Implicit					
	sd-wan	all	all	Source IP	any

2. Run the following CLI command:

```

# diagnose sys sdwan service

Service(1): Address Mode(IPV4) flags=0x0
Gen(1), TOS(0x0/0x0), Protocol(6: 80->80), Mode(manual)
Members:
  1: Seq_num(2 FGT_AWS_Tun), alive, selected
Src address:
  0.0.0.0-255.255.255.255
Dst address:
  10.0.2.0-10.0.2.255

```



```

Service(2): Address Mode(IPV4) flags=0x0
  Gen(1), TOS(0x0/0x0), Protocol(6: 22->22), Mode(manual)
  Members:
    1: Seq_num(1 AWS_VPG), alive, selected
  Src address:
    0.0.0.0-255.255.255.255
  Dst address:
    10.0.2.0-10.0.2.255

Service(3): Address Mode(IPV4) flags=0x0
  Gen(1), TOS(0x0/0x0), Protocol(6: 443->443), Mode(manual)
  Members:
    1: Seq_num(2 FGT_AWS_Tun), alive, selected
  Src address:
    0.0.0.0-255.255.255.255
  Dst address:
    10.0.2.0-10.0.2.255

Service(4): Address Mode(IPV4) flags=0x0
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members:
    1: Seq_num(1 AWS_VPG), alive, selected
  Src address:
    0.0.0.0-255.255.255.255
  Dst address:
    10.0.2.21-10.0.2.21

```

To verify that sessions are going to the correct tunnel:

1. Run the following CLI command to verify that HTTPS and HTTP traffic destined for the Web server at 10.0.2.20 uses FGT_AWS_Tun:

```

# diagnose sys session filter dst 10.0.2.20
# diagnose sys session list

session info: proto=6 proto_state=11 duration=2 expire=3597 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=FGT_AWS_Tun/ vlan_cos=0/255
state=log may_dirty npu f00 csf_syncd_log app_valid
statistic(bytes/packets/allow_err): org=593/4/1 reply=3689/5/1 tuples=3
tx speed(Bps/kbps): 264/2 rx speed(Bps/kbps): 1646/13
orgin->sink: org pre->post, reply pre->post dev=0->18/18->0 gwy=172.16.200.1/0.0.0.0
hook=post dir=org act=snat 10.100.88.101:55589->10.0.2.20:80(172.16.200.2:55589)
hook=pre dir=reply act=dnat 10.0.2.20:80->172.16.200.2:55589(10.100.88.101:55589)
hook=post dir=reply act=noop 10.0.2.20:80->10.100.88.101:55589(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=00:09:0f:00:03:01
misc=0 policy_id=32 auth_info=0 chk_client_info=0 vd=0
serial=00b7442c tos=ff/ff app_list=2000 app=34050 url_cat=0
rpd_b_link_id= ff000001 rpd_b_svc_id=2154552596 ngfwid=n/a
npu_state=0x3041008

```

```

session info: proto=6 proto_state=66 duration=1 expire=3 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=FGT_AWS_Tun/ vlan_cos=0/255
state=log may_dirty ndr f00 csf_syncd_log
statistic(bytes/packets/allow_err): org=48/1/0 reply=40/1/1 tuples=3
tx speed(Bps/kbps): 26/0 rx speed(Bps/kbps): 22/0
origin->sink: org pre->post, reply pre->post dev=5->18/18->5
gwy=172.16.200.1/10.100.88.101
hook=post dir=org act=snat 10.100.88.101:55621->10.0.2.20:443(172.16.200.2:55621)
hook=pre dir=reply act=dnat 10.0.2.20:443->172.16.200.2:55621(10.100.88.101:55621)
hook=post dir=reply act=noop 10.0.2.20:443->10.100.88.101:55621(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=00:09:0f:00:03:01
misc=0 policy_id=32 auth_info=0 chk_client_info=0 vd=0
serial=00b74b50 tos=ff/ff app_list=2000 app=0 url_cat=0
rpd_b_link_id= ff000003 rpd_b_svc_id=2154552596 ngfwid=n/a
npu_state=0x3041008

```

2. Run the following CLI command to verify that SSH and FTP traffic destined for the FTP server at 10.0.2.21 uses AWS_VPG:

```

# diagnose sys session filter dst 10.0.2.20
# diagnose sys session list

```

```

session info: proto=6 proto_state=11 duration=197 expire=3403 timeout=3600
flags=00000000 socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=AWS_VPG/ helper=ftp vlan_cos=0/255
state=log may_dirty ndr npu f00 csf_syncd_log app_valid
statistic(bytes/packets/allow_err): org=580/12/1 reply=863/13/1 tuples=3
tx speed(Bps/kbps): 2/0 rx speed(Bps/kbps): 4/0
origin->sink: org pre->post, reply pre->post dev=5->17/17->5
gwy=169.254.55.153/10.100.88.101
hook=post dir=org act=snat 10.100.88.101:55528->10.0.2.21:21(169.254.55.154:55528)
hook=pre dir=reply act=dnat 10.0.2.21:21->169.254.55.154:55528(10.100.88.101:55528)
hook=post dir=reply act=noop 10.0.2.21:21->10.100.88.101:55528(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=00:09:0f:00:03:01
misc=0 policy_id=32 auth_info=0 chk_client_info=0 vd=0
serial=00b72a5f tos=ff/ff app_list=2000 app=15896 url_cat=0
rpd_b_link_id= ff000004 rpd_b_svc_id=2149689849 ngfwid=n/a
npu_state=0x3041008

```

```

session info: proto=6 proto_state=11 duration=3 expire=3596 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=AWS_VPG/ vlan_cos=0/255
state=log may_dirty ndr npu f00 csf_syncd_log app_valid
statistic(bytes/packets/allow_err): org=1496/6/1 reply=1541/5/1 tuples=3
tx speed(Bps/kbps): 416/3 rx speed(Bps/kbps): 429/3

```

```

origin->sink: org pre->post, reply pre->post dev=5->17/17->5
gwy=169.254.55.153/10.100.88.101
hook=post dir=org act=snat 10.100.88.101:55644->10.0.2.21:22(169.254.55.154:55644)
hook=pre dir=reply act=dnat 10.0.2.21:22->169.254.55.154:55644(10.100.88.101:55644)
hook=post dir=reply act=noop 10.0.2.21:22->10.100.88.101:55644(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=00:09:0f:00:03:01
misc=0 policy_id=32 auth_info=0 chk_client_info=0 vd=0
serial=00b75287 tos=ff/ff app_list=2000 app=16060 url_cat=0
rpd_b_link_id= ff000002 rpd_b_svc_id=2149689849 ngfwid=n/a
npu_state=0x3041008

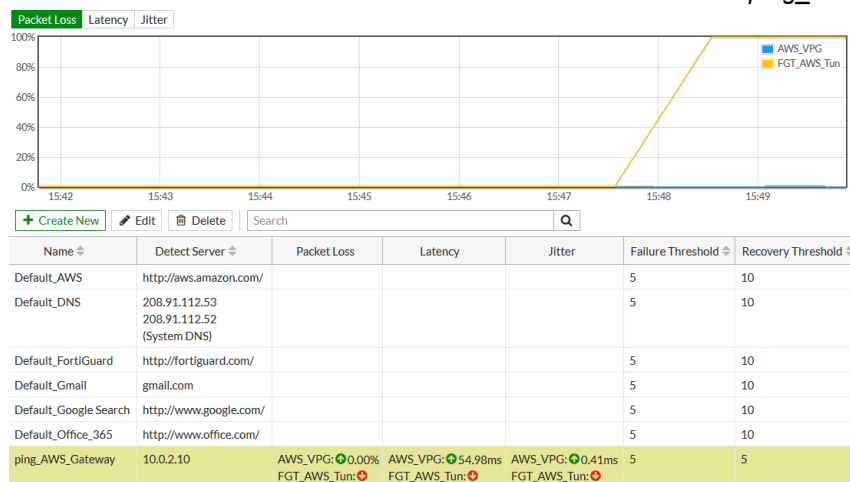
```

To simulate an issue on an overlay VPN tunnel:

On the cloud FortiGate-VM, disable the firewall policy allowing Core_Dialup to port2.

1. Health-checks through the FGT_AWS_Tun tunnel fail:

a. Go to *Network > Performance SLA* and select *Packet Loss* and the *ping_AWS_Gateway* SLA:



b. Run the following CLI command:

```

# diagnose sys sdwan health-check
...
Seq(1 AWS_VPG): state(alive), packet-loss(0.000%) latency(52.746), jitter(0.713) sla_map=0x0
Seq(2 FGT_AWS_Tun): state(dead), packet-loss(19.000%) sla_map=0x0

```

2. Service rules show that the member is down:

a. Go to *Network > SD-WAN Rules*:

ID	Name	Source	Destination	Criteria	Members	Hit Count
IPv4						
1	http-to-FGT_AWS_Tun	all	remote_subnet_10.0.2.0		FGT_AWS_Tun	1
2	ssh-to-AWS_VPG	all	remote_subnet_10.0.2.0		AWS_VPG	2
3	https-to-FGT_AWS_Tun	all	remote_subnet_10.0.2.0		FGT_AWS_Tun	1
4	ftp-to-AWS_VPG	all	FTP-Server		AWS_VPG	2
Implicit						
	sd-wan	all	all	Source IP	any	

b. Run the following CLI command:

```
# diagnose sys sdwan service
```

```

Service(1): Address Mode(IPV4) flags=0x0
  Gen(2), TOS(0x0/0x0), Protocol(6: 80->80), Mode(manual)
  Members:
    1: Seq_num(2 FGT_AWS_Tun), dead
  Src address:
    0.0.0.0-255.255.255.255
  Dst address:
    10.0.2.0-10.0.2.255

Service(2): Address Mode(IPV4) flags=0x0
  Gen(1), TOS(0x0/0x0), Protocol(6: 22->22), Mode(manual)
  Members:
    1: Seq_num(1 AWS_VPG), alive, selected
  Src address:
    0.0.0.0-255.255.255.255
  Dst address:
    10.0.2.0-10.0.2.255

Service(3): Address Mode(IPV4) flags=0x0
  Gen(2), TOS(0x0/0x0), Protocol(6: 443->443), Mode(manual)
  Members:
    1: Seq_num(2 FGT_AWS_Tun), dead
  Src address:
    0.0.0.0-255.255.255.255
  Dst address:
    10.0.2.0-10.0.2.255

Service(4): Address Mode(IPV4) flags=0x0
  Gen(1), TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
  Members:
    1: Seq_num(1 AWS_VPG), alive, selected
  Src address:
    0.0.0.0-255.255.255.255
  Dst address:
    10.0.2.21-10.0.2.21

```

3. Sessions are redirected to the working tunnel:

a. Run the following CLI command:

```

# diagnose sys session list

session info: proto=6 proto_state=11 duration=3 expire=3596 timeout=3600
flags=00000000 socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=AWS_VPG/ vlan_cos=0/255
state=log may_dirty ndr npu f00 csf_syncd_log app_valid
statistic(bytes/packets/allow_err): org=504/4/1 reply=620/3/1 tuples=3
tx speed(Bps/kbps): 150/1 rx speed(Bps/kbps): 184/1
origin->sink: org pre->post, reply pre->post dev=0->17/17->0
gwy=169.254.55.153/0.0.0.0
hook=post dir=org act=snat 10.100.88.101:56373->10.0.2.20:80(169.254.55.154:56373)
hook=pre dir=reply act=dnat 10.0.2.20:80->169.254.55.154:56373(10.100.88.101:56373)
hook=post dir=reply act=noop 10.0.2.20:80->10.100.88.101:56373(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)

```

```

src_mac=00:09:0f:00:03:01
misc=0 policy_id=32 auth_info=0 chk_client_info=0 vd=0
serial=00b87199 tos=ff/ff app_list=2000 app=34050 url_cat=0
rpd_b_link_id= 80000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x3041008

session info: proto=6 proto_state=66 duration=3 expire=1 timeout=3600 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=AWS_VPG/ vlan_cos=0/255
state=log may_dirty ndr f00 csf_syncd_log
statistic(bytes/packets/allow_err): org=48/1/0 reply=40/1/1 tuples=3
tx speed(Bps/kbps): 15/0 rx speed(Bps/kbps): 12/0
origin->sink: org pre->post, reply pre->post dev=5->17/17->5
gwy=169.254.55.153/10.100.88.101
hook=post dir=org act=snat 10.100.88.101:56383->10.0.2.20:443(169.254.55.154:56383)
hook=pre dir=reply act=dnat 10.0.2.20:443->169.254.55.154:56383(10.100.88.101:56383)
hook=post dir=reply act=noop 10.0.2.20:443->10.100.88.101:56383(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=00:09:0f:00:03:01
misc=0 policy_id=32 auth_info=0 chk_client_info=0 vd=0
serial=00b876bb tos=ff/ff app_list=2000 app=0 url_cat=0
rpd_b_link_id= 80000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x3041008
total session 2

```

4. Routes to the *FGT_AWS_Tun* tunnel are removed:

- a. If *Optimal* dashboards is selected, go to *Dashboard > Network* and expand the Routing widget to view the routing table.

If *Comprehensive* dashboards is selected, go to *Dashboard > Routing Monitor* and select *Static & Dynamic* in the widget toolbar to view the routing table:

Network ⇅	Gateway IP ⇅	Interfaces ⇅	Distance ⇅	IP Version ⇅	Type ⇅
IPv4 40					
0.0.0.0/0	10.100.64.254	Internet_A (port1)	1	IPv4	Static
0.0.0.0/0	10.100.65.254	Internet_B (port5)	1	IPv4	Static
10.0.2.0/24	169.254.55.153	AWS_VPG	1	IPv4	Static
10.0.10.0/24	0.0.0.0	VPN_A_Tunnel (Branch-HQ-A)	0	IPv4	Connected
10.0.10.1/32	0.0.0.0	VPN_A_Tunnel (Branch-HQ-A)	0	IPv4	Connected

- b. Run the following CLI command:

```

# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 10.100.64.254, port1

```

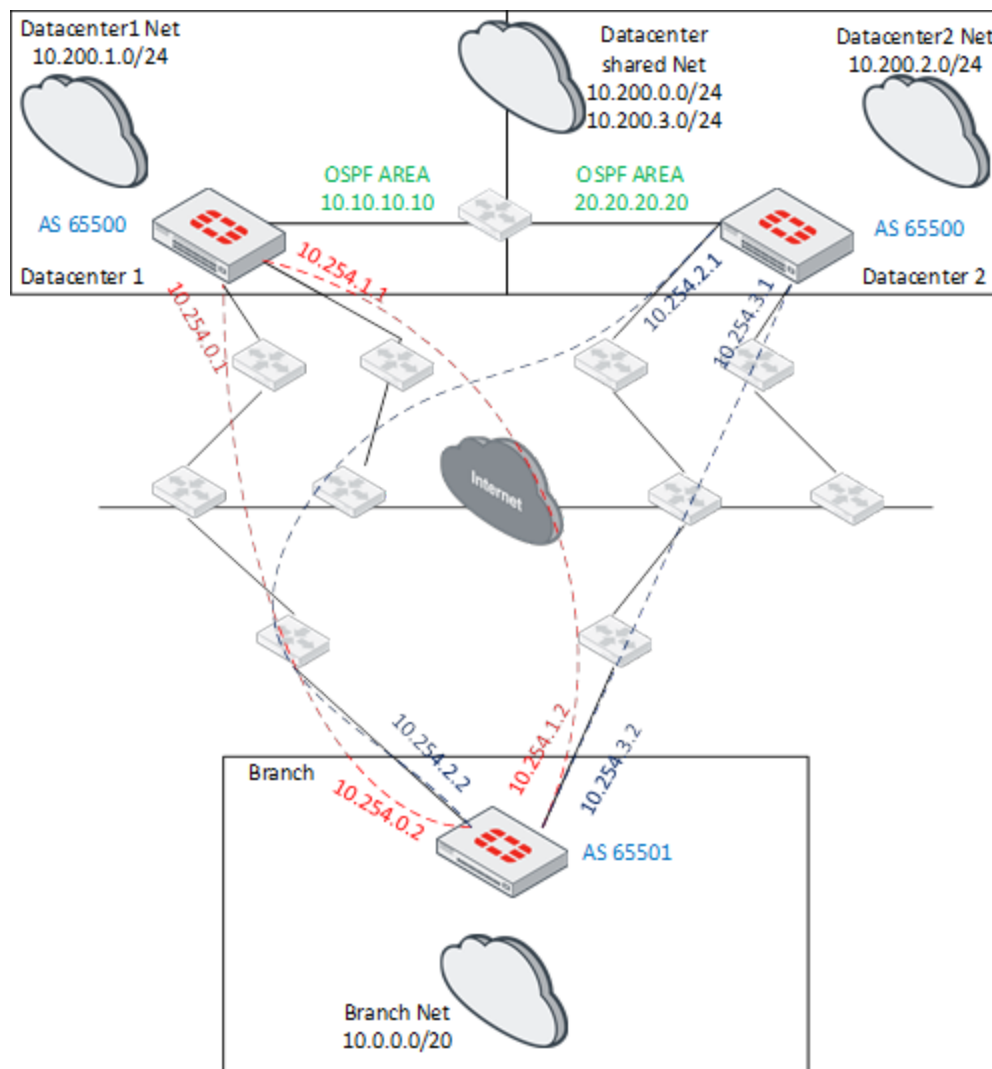
```

[1/0] via 10.100.65.254, port5
S    10.0.2.0/24 [1/0] via 169.254.55.153, AWS_VPG
C    10.0.10.0/24 is directly connected, Branch-HQ-A
C    10.0.10.1/32 is directly connected, Branch-HQ-A
...

```

Hub and spoke SD-WAN deployment example

This topology diagram shows an overview of the network that is configured in this example:



Datacenter configuration

The datacenter is configured to support:

- Zero touch provisioning of new spokes
- Point to multipoint VPN
- Central management of access with the datacenter firewall
- Dynamic peering, to share routing information between branches and the datacenter
- VDOM compatibility, with inter-VDOM links for isolation and segmentation

To configure the datacenter, complete the following steps:

1. [Configure dial-up \(dynamic\) VPN](#)
2. [Configure VPN interfaces](#)
3. [Configure loopback interface](#)
4. [Configure BGP](#)
5. [Firewall policies](#)
6. [Configure a black hole route](#)

Configure dial-up (dynamic) VPN

Dial-up, or dynamic, VPNs are used to facilitate zero touch provisioning of new spokes to establish VPN connections to the hub FortiGate.

The `exchange-interface-ip` option is enabled to allow the exchange of IPsec interface IP addresses. This allows a point to multipoint connection to the hub FortiGate.

The `add-route` option is disabled to allow multiple dial-up tunnels to be established to the same host that is advertising the same network. This dynamic network discovery is facilitated by the BGP configuration; see [Configure BGP on page 587](#) for details.

Wildcard security associations are defined for the phase2 interface because routing is used to determine if traffic is subject to encryption and transmission through the IPsec VPN tunnel. The phase1 interface name must be 11 characters or less.

A dynamic VPN configuration must be defined for each interface that connects to the internet.

To configure the IPsec phase1 interfaces:

```
config vpn ipsec phase1-interface
  edit "vpn-isp-a"
    set type dynamic
    set interface "port2"
    set peertype any
    set exchange-interface-ip enable
    set proposal aes256-sha256
    set add-route disable
    set dhgrp 5
    set net-device enable
    set psksecret *****
```

```
next
edit "vpn-isp-b"
    set type dynamic
    set interface "port3"
    set peertype any
    set exchange-interface-ip enable
    set proposal aes256-sha256
    set add-route disable
    set dhgrp 5
    set net-device enable
    set psksecret *****
next
end
```

To configure the IPsec phase2 interfaces:

```
config vpn ipsec phase2-interface
    edit "vpn-isp-a_p2"
        set phasename "vpn-isp-a"
        set proposal aes256-sha256
        set pfs disable
        set replay disable
    next
    edit "vpn-isp-b_p2"
        set phasename "vpn-isp-b"
        set proposal aes256-sha256
        set pfs disable
        set replay disable
    next
end
```

Configure VPN interfaces

To establish the BGP session, IP addresses must be assigned to the tunnel interfaces that BGP will use to peer.

The hub IP address is set to the address that the tunnels connect to. The remote IP address is set to highest unused IP address that is part of the tunnel network. This establishes two connected routes directly back to the branch FortiGate in the hub FortiGate's routing table.

Ping is allowed on the virtual interface to confirm that a point to point tunnel has been established between the hub and branch FortiGates.

To define IP addresses for VPN interfaces:

```
config system interface
    edit "vpn-isp-a"
        set vdom "root"
        set ip 10.254.0.1 255.255.255.255
        set allowaccess ping
        set type tunnel
        set remote-ip 10.254.0.254 255.255.255.0
        set interface "port2"
    next
    edit "vpn-isp-b"
        set vdom "root"
```

```
        set ip 10.254.1.1 255.255.255.255
        set allowaccess ping
        set type tunnel
        set remote-ip 10.254.1.254 255.255.255.0
        set interface "port3"
    next
end
```

Configure loopback interface

A loopback interface must be defined on the hub FortiGate to be used as a common probe point for the FortiGates that are using SD-WAN. The FortiGates send a probe packet from each of their SD-WAN member interfaces so that they can determine the best route according to their policies. Ping is allowed so that it can be used for measurements.

To configure the loopback interface on the hub FortiGate:

```
config system interface
    edit "loopback_0"
        set vdom "root"
        set ip 10.255.255.1 255.255.255.255
        set allowaccess ping
        set type loopback
    next
end
```

Configure BGP

Network route discovery is facilitated by BGP.

EBGP is used to prevent the redistribution of routes that are in the same Autonomous System (AS) number as the host. It is also required to influence route selection on the branches with AS-Path prepending. EBGP multipath is enabled so that the hub FortiGate can dynamically discover multiple paths for networks that are advertised at the branches.

The neighbor range and group settings are configured to allow peering relationships to be established without defining each individual peer. Connecting branches have their tunnel interfaces configured within the range of the BGP peer.

In order to facilitate the fastest route failovers, configure the following timers to their lowest levels: `scan-time`, `advertisement-interval`, `keep-alive-timer`, and `holdtime-timer`.

To configure BGP on the hub FortiGate:

```
config router bgp
    set as 65500
    set router-id 10.10.0.1
    set ebgp-multipath enable
    set graceful-restart enable
    config neighbor-group
        edit "branch-peers-1"
            set soft-reconfiguration enable
            set remote-as 65501
        next
        edit "branch-peers-2"
            set soft-reconfiguration enable
```

```

        set remote-as 65501
    next
end
config neighbor-range
    edit 1
        set prefix 10.254.0.0 255.255.255.0
        set neighbor-group "branch-peers-1"
    next
    edit 2
        set prefix 10.254.1.0 255.255.255.0
        set neighbor-group "branch-peers-2"
    next
end
config network
    edit 1
        set prefix 10.200.1.0 255.255.255.0
    next
    edit 2
        set prefix 10.200.0.0 255.255.255.0
    next
    edit 3
        set prefix 10.200.3.0 255.255.255.0
    next
end
end

```

Firewall policies

Centralized access is controlled from the hub FortiGate using Firewall policies. In addition to layer three and four inspection, security policies can be used in the policies for layer seven traffic inspection.

It is best practice to only allow the networks and services that are required for communication through the firewall. The following rules are the minimum that must be configured to allow SD-WAN to function:

Source Interface	Destination Interface	Source Address	Destination Address	Action	Schedule	Service	Comments
<vpn interfaces>	<internal Interface>	<branch tunnel IP addresses>	<hub FortiGate internal interface>	Accept	Always	ICMP	Allow health checks to the hub FortiGate
<vpn interfaces>	<internal Interface>	<branch networks>	<datacenter networks>	Accept	Always	<allowed services>	Allow traffic from branch networks

For this example, a simple policy that allows all traffic is configured.

To configure a firewall policy:

```

config firewall policy
    edit 1
        set name "Allow All"
        set srcintf "any"
    
```

```
        set dstintf "any"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

Configure a black hole route

If there is a temporary loss of connectivity to the branch routes, it is best practice to send the traffic that is destined for those networks into a black hole until connectivity is restored.

To configure a black hole route for branch networks:

```
config router static
    edit 6
        set dst 10.0.0.0/14
        set distance 254
        set blackhole enable
    next
end
```

Branch configuration

The branches are configured to support:

- Client side SD-WAN with intelligent load balancing based on link quality
- Easy to create configuration templates for quick spoke deployment
- Split tunnel deployment for local internet access
- VDOM compatibility, with inter-VDOM links for isolation and segmentation

To configure a branch, complete the following steps:

1. [Configure VPN to the hub](#)
2. [Configure VPN interfaces](#)
3. [Configure BGP](#)
4. [Configure SD-WAN](#)
5. [Firewall configuration](#)

Configure VPN to the hub

The branch uses a normal site-to-site VPN configuration.

Wildcard security associations are defined in the phase2 configuration because dynamic routing with BGP determines what traffic must traverse the VPN tunnel for encryption/transmission.

To make sure that the VPN is established, `auto-negotiate` is enabled.

To configure the IPsec phase1 interfaces:

```
config vpn ipsec phase1-interface
  edit "vpn_dc1-1"
    set interface "port2"
    set peertype any
    set exchange-interface-ip enable
    set proposal aes256-sha256
    set dhgrp 5
    set remote-gw 172.16.0.78
    set psksecret *****
  next
  edit "vpn_dc1-2"
    set interface "port3"
    set peertype any
    set exchange-interface-ip enable
    set proposal aes256-sha256
    set dhgrp 5
    set remote-gw 172.16.0.82
    set psksecret *****
  next
end
```

To configure the IPsec phase2 interfaces:

```
config vpn ipsec phase2-interface
  edit "vpn_dc1-1_p2"
    set phase1name "vpn_dc1-1"
    set proposal aes256-sha256
    set pfs disable
    set replay disable
    set auto-negotiate enable
  next
  edit "vpn_dc1-2_p2"
    set phase1name "vpn_dc1-2"
    set proposal aes256-sha256
    set pfs disable
    set replay disable
    set auto-negotiate enable
  next
end
```

Configure VPN interfaces

The branch must define its local tunnel interface IP address, and the remote tunnel interface IP address of the datacenter FortiGate, to establish the point to multipoint VPN.

To define IP addresses for VPN interfaces:

```
config system interface
  edit "vpn_dc1-1"
    set vdom "root"
    set ip 10.255.0.2 255.255.255.255
    set allowaccess ping
    set type tunnel
    set remote-ip 10.255.0.1 255.255.255.255
    set interface "port2"
  next
  edit "vpn_dc1-2"
    set vdom "root"
    set ip 10.255.1.2 255.255.255.255
    set allowaccess ping
    set type tunnel
    set remote-ip 10.255.1.1 255.255.255.255
    set interface "port3"
  next
end
```

Configure BGP

BGP enables learning dynamic routes from the datacenter. The BGP configuration is normal, with the definition of the datacenter FortiGate tunnel IP addresses set as BGP peers.

Routes that have the same network mask, administrative distance, priority, and AS length are automatically considered for SD-WAN when the interfaces that those routes are on are added to the SD-WAN interface group.

In order to facilitate the fastest route failovers, configure the following timers to their lowest levels: `scan-time`, `advertisement-interval`, `keep-alive-timer`, and `holdtime-timer`.

The `distance-external` option might need to be configured if you need routes that are learned from BGP to take precedence over static routes.

To configure BGP on the branch FortiGate:

```
config router bgp
  set as 65501
  set router-id 10.254.0.2
  set ebgp-multipath enable
  config neighbor
    edit "10.254.0.1"
      set soft-reconfiguration enable
      set remote-as 65500
    next
    edit "10.254.1.1"
      set soft-reconfiguration enable
      set remote-as 65500
    next
  end
end
```

Configure SD-WAN

SD-WAN configuration is required to load balance based on the quality of the links. It can be configured to select the best link based on characteristics such as jitter, packet loss, and latency. A policy route is created by the FortiGate to select the best link based on the defined criteria.

For SD-WAN interfaces, or members, the peer is defined to reference the BGP neighbor that is tied to that specific interface.

The health check is the ping server that gathers the link characteristics used for link selection. It is recommended that the minimum `failtime` be set to 2.

The service definition defines the criteria for the policy routes. It can match based on the following characteristics:

- Protocol
- Destination Address
- Source Address
- Identity Based Group
- Internet Service Definition
- Source Port
- Destination Port
- Destination Route Tag

To dynamically determine the networks of the policy routes, routes that are learned from a BGP neighbor are matched against a route map, and a tag is defined for the matching routes. The service rules learn the networks based on these tags, instead of defining objects based on the learned addresses' network prefixes. See [Dynamic definition of SD-WAN routes on page 596](#) for details on configuring the FortiGate to use the destination tags for the SD-WAN service definition.

To define the SD-WAN member interfaces:

```
config system virtual-wan-link
    set status enable
    config members
        edit 1
            set interface "vpn_dc1-1"
        next
        edit 2
            set interface "vpn_dc1-2"
        next
    end
end
```

To define the SD-WAN health checks:

```
config system virtual-wan-link
    config health-check
        edit "datacenter1"
            set server "10.200.1.1"
            set interval 1
            set failtime 2
            set recoverytime 10
        next
    end
end
```

To define the SD-WAN service rules:

```
config system virtual-wan-link
    config service
        edit 1
            set mode priority
            set dst n-corporate
            set health-check "datacenter1"
            set priority-members 1 2
        next
    end
end
```

Firewall configuration

Centralized access is controlled from the hub FortiGate using Firewall policies. In addition to layer three and four inspection, security policies can be used in the policies for layer seven traffic inspection.

It is best practice to only allow the networks and services that are required for communication through the firewall. The following rules are the minimum that must be configured to allow SD-WAN to function:

Source Interface	Destination Interface	Source Address	Destination Address	Action	Schedule	Service	Comments
<internal interface>	<virtual wan link>	<branch networks>	<datacenter networks>	Accept	Always	<allowed services>	Allow traffic from branch to datacenter
<virtual wan link>	<internal Interface>	<datacenter networks>	<branch networks>	Accept	Always	<allowed services>	Allow traffic from datacenter to branch

For this example, a simple policy that allows all traffic is configured.

To configure a firewall policy:

```
config firewall policy
  edit 1
    set name "Allow All"
    set srcintf "any"
    set dstintf "any"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
  next
end
```


Validation

The following commands can be used to validate the connections on the datacenter and branches.

Datacenter

Routing table:

```
get router info routing-table all
```

VPN establishment:

```
diagnose vpn ike gateway list
```

Branch

SD-WAN validation:

```
diagnose sys virtual-wan-link member
```

```
diagnose sys virtual-wan-link service
```

```
diagnose sys virtual-wan-link health-check
```

Routing table:

```
get router info routing-table all
```

```
get router info route-map-address
```

```
get router info bgp route-map <route-map-name>
```

VPN establishment:

```
diagnose vpn ike gateway list
```

Dynamic definition of SD-WAN routes

Dynamic definitions of SD-WAN routes alleviate administrators from needing to know the destination of the traffic that is being load balanced, which, in an environment where routes are constantly added and removed, required a significant amount of administrative overhead.

The FortiGate can be configured to apply a route map to a BGP neighbor, and tag the routes that are learned from that neighbor with the `set-route-tag` command. After those routes are assigned a tag ID in the route map, the ID can be referenced in the SD-WAN rule.

To define the route map to apply to the BGP neighbor:

```
config router route-map
  edit "map-comm1"
    config rule
      edit 1
        set match-origin igp
        set set-route-tag 12
      next
      edit 2
        set match-ip-address "pf-all-in"
        set set-route-tag 11
      next
    end
  next
end
```

To apply the route map to the BGP neighbor:

```
config router bgp
  config neighbor
    edit "10.254.0.1"
      set route-map-in "map-comm1"
    next
  end
end
```

To reference tagged routes in an SD-WAN rule:

```
config system virtual-wan-link
  config service
    edit 1
      set mode priority
      set dst-tag 11
      set health-check "datacenter1"
      set priority-members 1 2
    next
  end
end
```

Adding another datacenter

Datacenter FortiGates should be configured to establish an OSPF neighbor relationship with the internal core router. This allows the dynamic redistribution of routes to the branches that are receiving updates from the datacenter FortiGates.

To ensure the fastest failover with OSPF, the following timers are set to their minimum levels: `spf-timers`, `hello-interval`, `dead-interval`.

Bi-directional forwarding is enabled to allow the fastest convergence time if there is a failure with a peering neighbor.

To configure OSPF:

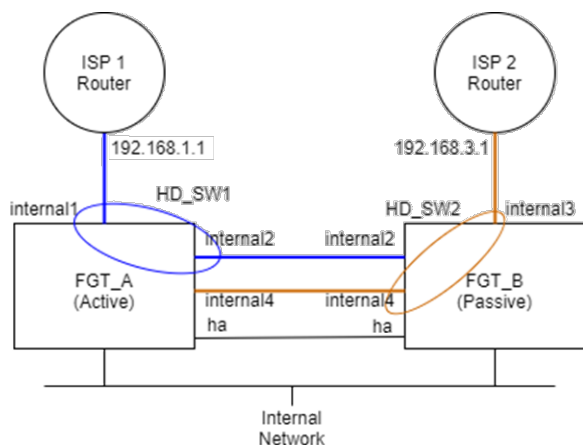
```
config router ospf
  set router-id 10.10.10.10
  set spf-timers 0 1
  set distribute-list-in "pf-datacenter2-tunnel"
  set restart-mode graceful-restart
  config area
    edit 10.10.10.10
    next
  end
  config ospf-interface
    edit "port5"
      set interface "port5"
      set dead-interval 3
      set hello-interval 1
      set bfd enable
    next
  end
  config network
    edit 1
      set prefix 192.168.100.0 255.255.255.252
      set area 10.10.10.10
    next
  end
  config redistribute "connected"
    set status enable
    set routemap "redistribute-branch-tunnel"
  end
  config redistribute "static"
  end
  config redistribute "rip"
  end
  config redistribute "bgp"
    set status enable
    set routemap "redistribute-branch-networks"
  end
  config redistribute "isis"
  end
end
```

Configuring SD-WAN in an HA cluster using internal hardware switches

In this SD-WAN configuration, two FortiGates in an active-passive (A-P) HA pair are used to provide hardware redundancy. Instead of using external switches to provide a mesh network connection to the ISP routers, the FortiGates use their built-in hardware switches to connect to the ISP routers.



Only FortiGate models that have hardware switches can be used for this solution. Ports in a software switch are not in a forwarding state when a FortiGate is acting as a secondary device in a A-P cluster.



In this topology:

- Two hardware switches are created, HD_SW1 and HD_SW2.
- HD_SW1 is used to connect to ISP 1 Router and includes the internal1 and internal2 ports.
- HD_SW2 is used to connect to ISP 2 Router and includes the internal3 and internal4 ports.
- Another interface on each device is used as the HA heartbeat interface, connecting the two FortiGates in HA.

The FortiGates create two hardware switches to connect to ISP 1 and ISP2. When FGT_A is the primary device, it reaches ISP 1 on internal1 in HD_SW1 and ISP 2 on internal4 in HD_SW2. When FGT_B is the primary device, it reaches ISP 1 on internal2 in HD_SW1 and ISP 2 on internal3 on HD_SW2.

HA failover

This is not a standard HA configuration with external switches. In the case of a device failure, one of the ISPs will no longer be available because the switch that is connected to it will be down.

For example, If FGT_A loses power, HA failover will occur and FGT_B will become the primary unit. Its connection to internal2 on HD_SW1 will also be down, so it will be unable to connect to ISP 1. Its SD-WAN SLAs will be broken, and traffic will only be routed through ISP 2.



A link on a hardware switch cannot be monitored in HA monitor, so it is impossible to perform link failure when a port in either of the hardware switches fails. Performing a link failure is unnecessary in this configuration though, because any link failure on the hardware switch will be experienced by both cluster members. SD-WAN SLA health checks should be used to monitor the health of each ISP.

Failure on a hardware switch or ISP router

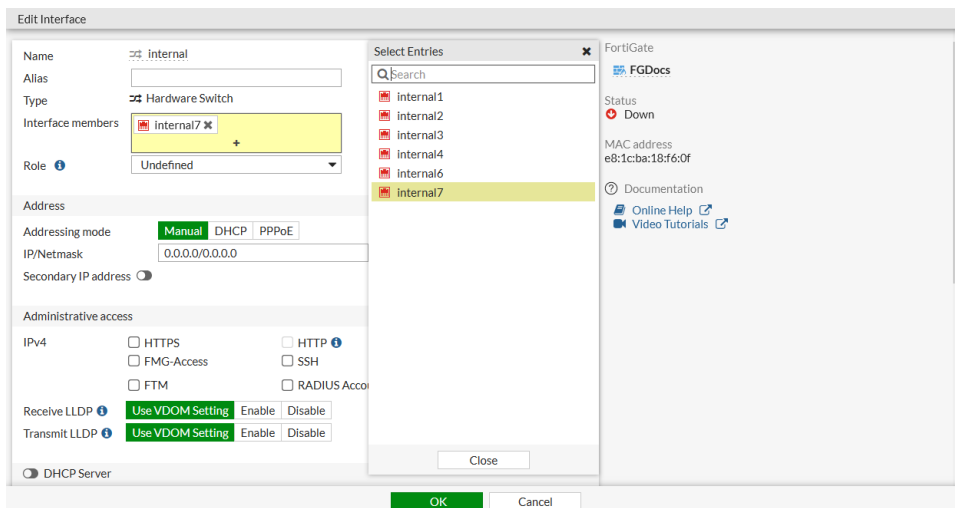
If a hardware switch or switch interface is down, or the ISP router is down, the SD-WAN can detect the broken SLA and continue routing to the other ISP.

For example, if FGT_A is the primary unit, and ISP 2 Router becomes unreachable, the SLA health checks on SD-WAN will detect the broken SLA and cause traffic to stop routing to ISP 2.

Configuration

To configure the HA A-P cluster with internal hardware switches:

1. Configure two FortiGates with internal switches in an A-P HA cluster (follow the steps in [HA active-active cluster setup on page 700](#)), starting by connecting the heartbeat interface.
2. When the HA cluster is up, connect to the primary FortiGate's GUI.
3. Remove the existing interface members from the default hardware switch:
 - a. Go to *Network > Interfaces*.
 - b. In the *LAN* section, double-click the *internal* interface to edit it.
 - c. In the *Interface Members* box, remove all but one of the interfaces.



- d. Click **OK**.
4. Configure the hardware switch interfaces for the two ISPs:
 - a. Go to *Network > Interfaces* and click *Create New > Interface*.
 - b. Enter a name (*HD_SW1*).
 - c. Set *Type* to *Hardware Switch*.

- d. In *Interface Members*, add two interfaces (*internal1* and *internal2*).
- e. Set *IP/Netmask* to *192.168.1.2/24*.
- f. Configure the remaining settings as needed.

The screenshot shows the 'New Interface' configuration window for a FortiGate device. The 'Name' field is set to 'HD_SW1'. The 'Type' is set to 'Hardware Switch'. Under 'Interface members', 'Internal1' and 'Internal2' are selected. The 'Role' is set to 'LAN'. In the 'Address' section, 'Addressing mode' is set to 'Manual', 'IP/Netmask' is '192.168.1.2/24', and 'Create address object matching subnet' is checked. The 'Name' of the address object is 'HD_SW1 address' and the 'Destination' is '192.168.1.2/24'. The 'Secondary IP address' is disabled. In the 'Administrative access' section, 'IPv4' is checked, and 'HTTPS', 'SSH', 'PING', 'SNMP', 'FTM', 'RADIUS Accounting', and 'Security Fabric Connection' are all unchecked. The 'OK' button is highlighted in green.

- g. Click **OK**.
- h. Repeat these steps to create a second hardware switch interface (*HD_SW2*) with two interface members (*internal3* and *internal4*) and *IP/Netmask* set to *192.168.3.2/24*.

The screenshot shows the 'New Interface' configuration window for a FortiGate device. The 'Name' field is set to 'HD_SW2'. The 'Type' is set to 'Hardware Switch'. Under 'Interface members', 'Internal3' and 'Internal4' are selected. The 'Role' is set to 'LAN'. In the 'Address' section, 'Addressing mode' is set to 'Manual', 'IP/Netmask' is '192.168.3.2/24', and 'Create address object matching subnet' is checked. The 'Name' of the address object is 'HD_SW2 address' and the 'Destination' is '192.168.3.2/24'. The 'Secondary IP address' is disabled. In the 'Administrative access' section, 'IPv4' is checked, and 'HTTPS', 'SSH', 'PING', 'SNMP', 'FTM', 'RADIUS Accounting', and 'Security Fabric Connection' are all unchecked. The 'OK' button is highlighted in green.

To connect the devices as shown in the topology:

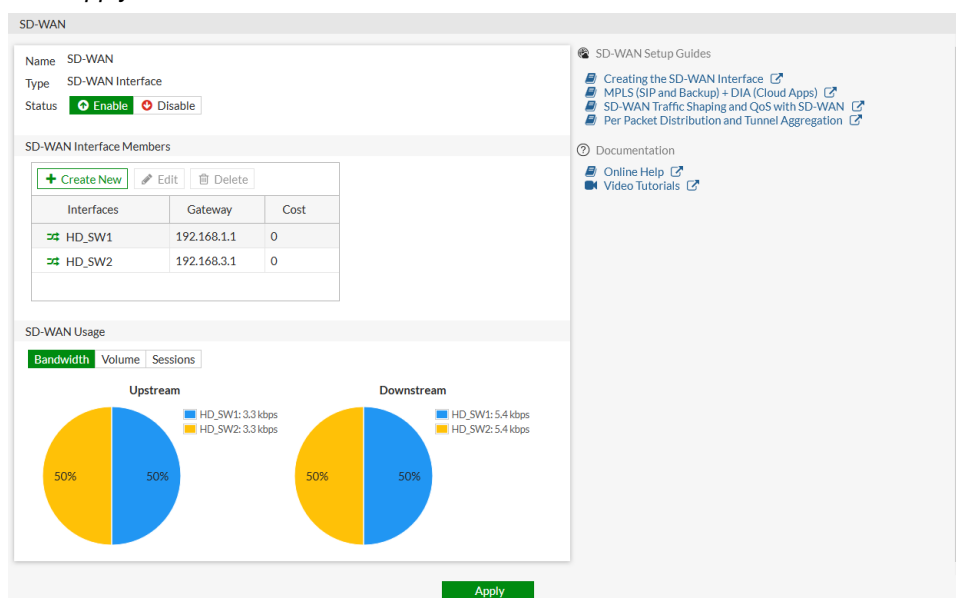
1. Connect the incoming interface to the internal switch on both FortiGates.
2. On FGT_A, connect internal1 of HD_SW1 to ISP 1 Router.
3. On FGT_B, connect internal3 of HD_SW2 to ISP 2 Router.
4. For HD_SW1, connect FGT_A internal2 directly to FGT_B internal2.
5. For HD_SW2, connect FGT_A internal4 directly to FGT_B internal4.

To configure SD-WAN:



The primary FortiGate makes all the SD-WAN decisions.

1. On the primary FortiGate, go to *Network > SD-WAN*.
2. Set *Status* to *Enable*.
3. In the *SD-WAN Interface Members* section, click *Create New*. The *New SD-WAN Member* pane opens.
4. In the *Interface* dropdown, select *HD_SW1* and enter the *Gateway* address *192.168.1.1*.
5. Click *OK*.
6. Repeat these steps to add the second interface (*HD_SW2*) with *Gateway* *192.168.3.1*.
7. Click *Apply*.



8. Create a health check:
 - a. Go to *Network > Performance SLA* and click *Create New*.
 - b. Set *Name* to *GW_HC*.
 - c. Set *Protocol* to *Ping* and *Servers* to *8.8.8.8*.
 - d. Set *Participants* to all of the SD-WAN members.
 - e. Add an *SLA Target* and leave the default values.
 - f. Click *OK*.
9. Create SD-WAN rules as needed. The SLA health check can be used to determine when the ISP connections are in or out of SLA, and to failover accordingly.

Troubleshooting SD-WAN

The following topics provide instructions on SD-WAN troubleshooting:

- Tracking SD-WAN sessions on page 602
- Understanding SD-WAN related logs on page 602
- SD-WAN related diagnose commands on page 605
- SLA logging on page 609
- SLA monitoring using the REST API on page 611
- SD-WAN bandwidth monitoring service on page 613

Tracking SD-WAN sessions

You can check the destination interface in *FortiView* in order to see which port the traffic is being forwarded to.

The example below demonstrates a source-based load-balance between two SD-WAN members.

- If the source IP address is an *even* number, it will go to *port13*.
- If the source IP address is an *odd* number, it will go to *port12*.

Source	Device	Destination	Application	Protocol	Source Port	Destination Port	Bytes	Duration (seconds)	Destination Interface
172.16.205.60	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	39803	80	60 B	5s	To_Juniper_ge-0/0/2 (port13)
172.16.205.13	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	47803	80	60 B	7s	port12
172.16.205.54	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	54011	80	60 B	1s	To_Juniper_ge-0/0/2 (port13)
172.16.205.37	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	46203	80	60 B	3s	port12
172.16.205.61	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	46203	80	60 B	9s	port12
172.16.205.36	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	37787	80	60 B	5s	To_Juniper_ge-0/0/2 (port13)
172.16.205.54	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	54171	80	60 B	8s	To_Juniper_ge-0/0/2 (port13)
172.16.205.100	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	38219	80	60 B	3s	To_Juniper_ge-0/0/2 (port13)
172.16.205.93	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	46331	80	60 B	5s	port12
172.16.205.86	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	54491	80	60 B	1s	To_Juniper_ge-0/0/2 (port13)
172.16.205.61	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	46667	80	60 B	7s	port12
172.16.205.61	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	46555	80	60 B	5s	port12
172.16.205.85	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	46555	80	60 B	8s	port12
172.16.205.93	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	46779	80	60 B	6s	port12
172.16.205.37	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	46747	80	60 B	1s	port12
172.16.205.100	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	36603	80	60 B		To_Juniper_ge-0/0/2 (port13)
172.16.205.13	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	45131	80	60 B	6s	port12
172.16.205.53	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	45003	80	60 B		port12
172.16.205.69	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	45019	80	60 B		port12
172.16.205.52	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	36827	80	60 B	4s	To_Juniper_ge-0/0/2 (port13)
172.16.205.101	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	45019	80	60 B	4s	port12
172.16.205.109	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	45371	80	60 B	9s	port12
172.16.205.84	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	37179	80	60 B	2s	To_Juniper_ge-0/0/2 (port13)
172.16.205.46	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	53563	80	60 B	7s	To_Juniper_ge-0/0/2 (port13)
172.16.205.108	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	37227	80	60 B	2s	To_Juniper_ge-0/0/2 (port13)
172.16.205.52	00:00:00:00:00:00	10.100.2.22	TCP80	TCP	37387	80	60 B	9s	To_Juniper_ge-0/0/2 (port13)

For information on other features of FortiView, see [FortiView on page 276](#).

Understanding SD-WAN related logs

This topic lists the SD-WAN related logs and explains when the logs will be triggered.

Health-check detects a failure:

- When health-check detects a failure, it will record a log:

```
34: date=2019-03-23 time=17:26:06 logid="0100022921" type="event" subtype="system"
level="critical" vd="root" eventtime=1553387165 logdesc="Routing information changed"
name="test" interface="R150" status="down" msg="Static route on interface R150 may be
removed by health-check test. Route: (10.100.1.2->10.100.2.22 ping-down) "
```

- When health-check detects a recovery, it will record a log:

```
32: date=2019-03-23 time=17:26:54 logid="0100022921" type="event" subtype="system"
level="critical" vd="root" eventtime=1553387214 logdesc="Routing information changed"
```



```
name="test" interface="R150" status="up" msg="Static route on interface R150 may be
added by health-check test. Route: (10.100.1.2->10.100.2.22 ping-up) "
```

Health-check has an SLA target and detects SLA qualification changes:

- When health-check has an SLA target and detects SLA changes, and changes to fail:

```
5: date=2019-04-11 time=11:48:39 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1555008519816639290 logdesc="Virtual WAN Link status"
msg="SD-WAN Health Check(ping) SLA(1): number of pass members changes from 2 to 1."
```

- When health-check has an SLA target and detects SLA changes, and changes to pass:

```
2: date=2019-04-11 time=11:49:46 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1555008586149038471 logdesc="Virtual WAN Link status"
msg="SD-WAN Health Check(ping) SLA(1): number of pass members changes from 1 to 2."
```

SD-WAN calculates a link's session/bandwidth over/under its ratio and stops/resumes traffic:

- When SD-WAN calculates a link's session/bandwidth over its configured ratio and stops forwarding traffic:

```
3: date=2019-04-10 time=17:15:40 logid="0100022924" type="event" subtype="system"
level="notice" vd="root" eventtime=1554941740185866628 logdesc="Virtual WAN Link volume
status" interface="R160" msg="The member(3) enters into conservative status with limited
ability to receive new sessions for too much traffic."
```

- When SD-WAN calculates a link's session/bandwidth according to its ratio and resumes forwarding traffic:

```
1: date=2019-04-10 time=17:20:39 logid="0100022924" type="event" subtype="system"
level="notice" vd="root" eventtime=1554942040196041728 logdesc="Virtual WAN Link volume
status" interface="R160" msg="The member(3) resume normal status to receive new sessions
for internal adjustment."
```

The SLA mode service rule's SLA qualified member changes:

- When the SLA mode service rule's SLA qualified member changes. In this example R150 fails the SLA check, but is still alive:

```
14: date=2019-03-23 time=17:44:12 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1553388252 logdesc="Virtual WAN Link status"
msg="Service2() prioritized by SLA will be redirected in seq-num order 2(R160) 1(R150). "
15: date=2019-03-23 time=17:44:12 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1553388252 logdesc="Virtual WAN Link status"
interface="R150" msg="The member1(R150) SLA order changed from 1 to 2. "
16: date=2019-03-23 time=17:44:12 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1553388252 logdesc="Virtual WAN Link status"
interface="R160" msg="The member2(R160) SLA order changed from 2 to 1. "
```

- When the SLA mode service rule's SLA qualified member changes. In this example R150 changes from fail to pass:

```
1: date=2019-03-23 time=17:46:05 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1553388365 logdesc="Virtual WAN Link status"
msg="Service2() prioritized by SLA will be redirected in seq-num order 1(R150) 2(R160). "
2: date=2019-03-23 time=17:46:05 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1553388365 logdesc="Virtual WAN Link status"
interface="R160" msg="The member2(R160) SLA order changed from 1 to 2. "
3: date=2019-03-23 time=17:46:05 logid="0100022923" type="event" subtype="system"
```

```
level="notice" vd="root" eventtime=1553388365 logdesc="Virtual WAN Link status"
interface="R150" msg="The member1(R150) SLA order changed from 2 to 1. "
```

The priority mode service rule member's link status changes:

- When priority mode service rule member's link status changes. In this example R150 changes to better than R160, and both are still alive:

```
1: date=2019-03-23 time=17:33:23 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1553387603 logdesc="Virtual WAN Link status"
msg="Service2() prioritized by packet-loss will be redirected in seq-num order 1(R150) 2
(R160). "
2: date=2019-03-23 time=17:33:23 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1553387603 logdesc="Virtual WAN Link status"
interface="R160" msg="The member2(R160) link quality packet-loss order changed from 1 to
2. "
3: date=2019-03-23 time=17:33:23 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1553387603 logdesc="Virtual WAN Link status"
interface="R150" msg="The member1(R150) link quality packet-loss order changed from 2 to
1. "
```

- When priority mode service rule member's link status changes. In this example R160 changes to better than R150, and both are still alive:

```
6: date=2019-03-23 time=17:32:01 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1553387520 logdesc="Virtual WAN Link status"
msg="Service2() prioritized by packet-loss will be redirected in seq-num order 2(R160) 1
(R150). "
7: date=2019-03-23 time=17:32:01 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1553387520 logdesc="Virtual WAN Link status"
interface="R150" msg="The member1(R150) link quality packet-loss order changed from 1 to
2. "
8: date=2019-03-23 time=17:32:01 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1553387520 logdesc="Virtual WAN Link status"
interface="R160" msg="The member2(R160) link quality packet-loss order changed from 2 to
1. "
```

SD-WAN member is used in service and it fails the health-check:

- When SD-WAN member fails the health-check, it will stop forwarding traffic:

```
6: date=2019-04-11 time=13:33:21 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1555014801844089814 logdesc="Virtual WAN Link status"
interface="R160" msg="The member2(R160) link is unreachable or miss threshold. Stop
forwarding traffic. "
```

- When SD-WAN member passes the health-check again, it will resume forwarding logs:

```
2: date=2019-04-11 time=13:33:36 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1555014815914643626 logdesc="Virtual WAN Link status"
interface="R160" msg="The member2(R160) link is available. Start forwarding traffic. "
```

Load-balance mode service rule's SLA qualified member changes:

- When load-balance mode service rule's SLA qualified member changes. In this example R150 changes to not meet SLA:

```

2: date=2019-04-11 time=14:11:16 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1555017075926510687 logdesc="Virtual WAN Link status"
msg="Service1(rule2) will be load balanced among members 2(R160) with available
routing."
3: date=2019-04-11 time=14:11:16 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1555017075926508676 logdesc="Virtual WAN Link status"
interface="R150" msg="The member1(R150) SLA order changed from 1 to 2. "
4: date=2019-04-11 time=14:11:16 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1555017075926507182 logdesc="Virtual WAN Link status"
interface="R160" msg="The member2(R160) SLA order changed from 2 to 1. "

```

- When load-balance mode service rule's SLA qualified member changes. In this example R150 changes to meet SLA:

```

1: date=2019-04-11 time=14:33:23 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1555017075926510668 logdesc="Virtual WAN Link status"
msg="Service1(rule2) will be load balanced among members 1(R150) 2(R160) with available
routing."
2: date=2019-03-23 time=14:33:23 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1553387603592651068 logdesc="Virtual WAN Link status"
interface="R160" msg="The member2(R160) link quality packet-loss order changed from 1 to
2. "
3: date=2019-03-23 time=14:33:23 logid="0100022923" type="event" subtype="system"
level="notice" vd="root" eventtime=1553387603592651068 logdesc="Virtual WAN Link status"
interface="R150" msg="The member1(R150) link quality packet-loss order changed from 2 to
1. "

```

SLA link status logs, generated with interval sla-fail-log-period or sla-pass-log-period:

- When SLA fails, SLA link status logs will be generated with interval sla-fail-log-period:

```

7: date=2019-03-23 time=17:45:54 logid="0100022925" type="event" subtype="system"
level="notice" vd="root" eventtime=1553388352 logdesc="Link monitor SLA information"
name="test" interface="R150" status="up" msg="Latency: 0.016, jitter: 0.002, packet
loss: 21.000%, inbandwidth: 0Mbps, outbandwidth: 200Mbps, bibandwidth: 200Mbps, sla_map:
0x0"

```

- When SLA passes, SLA link status logs will be generated with interval sla-pass-log-period:

```

5: date=2019-03-23 time=17:46:05 logid="0100022925" type="event" subtype="system"
level="information" vd="root" eventtime=1553388363 logdesc="Link monitor SLA
information" name="test" interface="R150" status="up" msg="Latency: 0.017, jitter:
0.003, packet loss: 0.000%, inbandwidth: 0Mbps, outbandwidth: 200Mbps, bibandwidth:
200Mbps, sla_map: 0x1"

```

SD-WAN related diagnose commands

This topic lists the SD-WAN related diagnose commands and related output.

To check SD-WAN health-check status:

```

FGT # diagnose sys virtual-wan-link health-check
Health Check(server):
Seq(1): state(alive), packet-loss(0.000%) latency(15.247), jitter(5.231) sla_map=0x0
Seq(2): state(alive), packet-loss(0.000%) latency(13.621), jitter(6.905) sla_map=0x0

```

```

FGT # diagnose sys virtual-wan-link health-check
Health Check(ping):
Seq(1): state(alive), packet-loss(0.000%) latency(0.683), jitter(0.082) sla_map=0x0
Seq(2): state(dead), packet-loss(100.000%) sla_map=0x0

FGT # diagnose sys virtual-wan-link health-check google
Health Check(google):
Seq(1): state(alive), packet-loss(0.000%) latency(14.563), jitter(4.334) sla_map=0x0
Seq(2): state(alive), packet-loss(0.000%) latency(12.633), jitter(6.265) sla_map=0x0

```

To check SD-WAN member status:

- When SD-WAN load-balance mode is *source-ip-based/source-dest-ip-based*.

```

FGT # diagnose sys virtual-wan-link member
Member(1): interface: port13, gateway: 10.100.1.1 2004:10:100:1::1, priority: 0, weight:
0
Member(2): interface: port15, gateway: 10.100.1.5 2004:10:100:1::5, priority: 0, weight:
0

```

- When SD-WAN load-balance mode is *weight-based*.

```

FGT # diagnose sys virtual-wan-link member
Member(1): interface: port13, gateway: 10.100.1.1 2004:10:100:1::1, priority: 0, weight:
33
Member(2): interface: port15, gateway: 10.100.1.5 2004:10:100:1::5, priority: 0, weight:
66

```

- When SD-WAN load-balance mode is *measured-volume-based*.

- Both members are under volume and still have room:

```

FGT # diagnose sys virtual-wan-link member
Member(1): interface: port13, gateway: 10.100.1.1 2004:10:100:1::1, priority: 0,
weight: 33
    Config volume ratio: 33, last reading: 8211734579B, volume room 33MB
Member(2): interface: port15, gateway: 10.100.1.5 2004:10:100:1::5, priority: 0,
weight: 66
    Config volume ratio: 66, last reading: 24548159B, volume room 66MB

```

- Some members are overloaded and some still have room:

```

FGT # diagnose sys virtual-wan-link member
Member(1): interface: port1, gateway: 10.10.0.2, priority: 0, weight: 0
    Config volume ratio: 10, last reading: 10297221000B, overload volume 1433MB
Member(2): interface: port2, gateway: 10.11.0.2, priority: 0, weight: 38
    Config volume ratio: 50, last reading: 45944239916B, volume room 38MB

```

- When SD-WAN load balance mode is *usage-based/spillover*.

- When no spillover occurs:

```

FGT # diagnose sys virtual-wan-link member
Member(1): interface: port13, gateway: 10.100.1.1 2004:10:100:1::1, priority: 0,
weight: 255
    Egress-spillover-threshold: 400kbit/s, ingress-spillover-threshold: 300kbit/s
    Egress-overbps=0, ingress-overbps=0
Member(2): interface: port15, gateway: 10.100.1.5 2004:10:100:1::5, priority: 0,
weight: 254
    Egress-spillover-threshold: 0kbit/s, ingress-spillover-threshold: 0kbit/s
    Egress-overbps=0, ingress-overbps=0

```

- When member has reached limit and spillover occurs:

```
FGT # diagnose sys virtual-wan-link member
Member(1): interface: port13, gateway: 10.100.1.1 2004:10:100:1::1, priority: 0,
weight: 255
    Egress-spillover-threshold: 400kbit/s, ingress-spillover-threshold: 300kbit/s
    Egress-overbps=1, ingress-overbps=1
Member(2): interface: port15, gateway: 10.100.1.5 2004:10:100:1::5, priority: 0,
weight: 254
    Egress-spillover-threshold: 0kbit/s, ingress-spillover-threshold: 0kbit/s
    Egress-overbps=0, ingress-overbps=0
```

- You can also use the `diagnose netlink dstmac list` command to check if you are over the limit.

```
FGT # diagnose netlink dstmac list port13
dev=port13 mac=08:5b:0e:ca:94:9d rx_tcp_mss=0 tx_tcp_mss=0 egress_overspill_
threshold=51200 egress_bytes=103710 egress_over_bps=1 ingress_overspill_
threshold=38400 ingress_bytes=76816 ingress_over_bps=1 sampler_rate=0
```

To check SD-WAN service rules status:

- *Manual mode* service rules.

```
FGT # diagnose sys virtual-wan-link service
Service(1): Address Mode(IPV4) flags=0x0
TOS(0x0/0x0), Protocol(0: 1->65535), Mode(manual)
Members:
    1: Seq_num(2), alive, selected
Dst address: 10.100.21.0-10.100.21.255
```

- *Auto mode* service rules.

```
FGT # diagnose sys virtual-wan-link service
Service(1): Address Mode(IPV4) flags=0x0
TOS(0x0/0x0), Protocol(0: 1->65535), Mode(auto), link-cost-factor(latency), link-cost-
threshold(10), health-check(ping)
Members:
    1: Seq_num(2), alive, latency: 0.011
    2: Seq_num(1), alive, latency: 0.018, selected
Dst address: 10.100.21.0-10.100.21.255
```

- *Priority mode* service rules.

```
FGT # diagnose sys virtual-wan-link service
Service(1): Address Mode(IPV4) flags=0x0
TOS(0x0/0x0), Protocol(0: 1->65535), Mode(priority), link-cost-factor(latency), link-
cost-threshold(10), health-check(ping)
Members:
    1: Seq_num(2), alive, latency: 0.011, selected
    2: Seq_num(1), alive, latency: 0.017, selected
Dst address: 10.100.21.0-10.100.21.255
```

- *Load-balance mode* service rules.

```
FGT # diagnose sys virtual-wan-link service
Service(1): Address Mode(IPV4) flags=0x0
TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance)
Members:
    1: Seq_num(1), alive, sla(0x1), num of pass(1), selected
```

```
2: Seq_num(2), alive, sla(0x1), num of pass(1), selected
Dst address: 10.100.21.0-10.100.21.255
```

- **SLA mode service rules.**

```
FGT # diagnose sys virtual-wan-link service
Service(1): Address Mode(IPV4) flags=0x0
TOS(0x0/0x0), Protocol(0: 1->65535), Mode(sla)
Members:
1: Seq_num(1), alive, sla(0x1), cfg_order(0), cost(0), selected
2: Seq_num(2), alive, sla(0x1), cfg_order(1), cost(0), selected
Dst address: 10.100.21.0-10.100.21.255
```

To check interface logs from the past 15 minutes:

```
FGT (root) # diagnose sys virtual-wan-link intf-sla-log R150
Timestamp: Fri Apr 12 11:08:36 2019, used inbandwidth: 0bps, used outbandwidth: 0bps, used
bibandwidth: 0bps, tx bytes: 860bytes, rx bytes: 1794bytes.
Timestamp: Fri Apr 12 11:08:46 2019, used inbandwidth: 1761bps, used outbandwidth: 1710bps,
used bibandwidth: 3471bps, tx bytes: 2998bytes, rx bytes: 3996bytes.
Timestamp: Fri Apr 12 11:08:56 2019, used inbandwidth: 2452bps, used outbandwidth: 2566bps,
used bibandwidth: 5018bps, tx bytes: 7275bytes, rx bytes: 7926bytes.
Timestamp: Fri Apr 12 11:09:06 2019, used inbandwidth: 2470bps, used outbandwidth: 3473bps,
used bibandwidth: 5943bps, tx bytes: 13886bytes, rx bytes: 11059bytes.
Timestamp: Fri Apr 12 11:09:16 2019, used inbandwidth: 2433bps, used outbandwidth: 3417bps,
used bibandwidth: 5850bps, tx bytes: 17946bytes, rx bytes: 13960bytes.
Timestamp: Fri Apr 12 11:09:26 2019, used inbandwidth: 2450bps, used outbandwidth: 3457bps,
used bibandwidth: 5907bps, tx bytes: 22468bytes, rx bytes: 17107bytes.
```

To check SLA logs in the past 15 minutes:

```
FGT (root) # diagnose sys virtual-wan-link sla-log ping 1
Timestamp: Fri Apr 12 11:09:27 2019, vdom root, health-check ping, interface: R150, status:
up, latency: 0.014, jitter: 0.003, packet loss: 16.000%.
Timestamp: Fri Apr 12 11:09:28 2019, vdom root, health-check ping, interface: R150, status:
up, latency: 0.015, jitter: 0.003, packet loss: 15.000%.
Timestamp: Fri Apr 12 11:09:28 2019, vdom root, health-check ping, interface: R150, status:
up, latency: 0.014, jitter: 0.003, packet loss: 14.000%.
Timestamp: Fri Apr 12 11:09:29 2019, vdom root, health-check ping, interface: R150, status:
up, latency: 0.015, jitter: 0.003, packet loss: 13.000%.
```

To check Application Control used in SD-WAN and the matching IP addresses:

```
FGT # diagnose sys virtual-wan-link internet-service-app-ctrl-list
Ctrl application(Microsoft.Authentication 41475):Internet Service ID(4294836224)
Protocol(6), Port(443)
Address(2): 104.42.72.21 131.253.61.96
Ctrl application(Microsoft.CDN 41470):Internet Service ID(4294836225)
Ctrl application(Microsoft.Lync 28554):Internet Service ID(4294836226)
Ctrl application(Microsoft.Office.365 33182):Internet Service ID(4294836227)
Ctrl application(Microsoft.Office.365.Portals 41468):Internet Service ID(4294836228)
Ctrl application(Microsoft.Office.Online 16177):Internet Service ID(4294836229)
Ctrl application(Microsoft.OneNote 40175):Internet Service ID(4294836230)
Ctrl application(Microsoft.Portals 41469):Internet Service ID(4294836231)
Protocol(6), Port(443)
Address(8): 23.58.134.172 131.253.33.200 23.58.135.29 204.79.197.200 64.4.54.254
```

```
23.59.156.241 13.77.170.218 13.107.22.200
Ctrl application(Microsoft.Sharepoint 16190):Internet Service ID(4294836232)
Ctrl application(Microsoft.Sway 41516):Internet Service ID(4294836233)
Ctrl application(Microsoft.Tenant.Namespace 41471):Internet Service ID(4294836234)
```

To check IPsec aggregate interface when SD-WAN uses the per-packet distribution feature:

```
# diagnose sys ipsec-aggregate list
agg1 algo=L3 member=2 run_tally=2
members:
    vdl-p1
    vdl-p2
```

To check BGP learned routes and determine if they are used in SD-WAN service:

```
FGT # get router info bgp network
FGT # get router info bgp network 10.100.11.0
BGP routing table entry for 10.100.10.0/24
Paths: (2 available, best 1, table Default-IP-Routing-Table)
    Advertised to non peer-group peers:
        172.10.22.2
    20
        10.100.20.2 from 10.100.20.2 (6.6.6.6)
            Origin EGP metric 200, localpref 100, weight 10000, valid, external, best
            Community: 30:5
            Last update: Wen Mar 20 18:45:17 2019
FGT # get router info route-map-address
Extend-tag: 15, interface(wan2:16)
    10.100.11.0/255.255.255.0

FGT # diagnose firewall proute list
list route policy info(vf=root):

id=4278779905 vwl_service=1(DataCenter) flags=0x0 tos=0x00 tos_mask=0x00 protocol=0
sport=0:65535 iif=0 dport=1-65535 oif=16
source wildcard(1): 0.0.0.0/0.0.0.0
destination wildcard(1): 10.100.11.0/255.255.255.0
```

SLA logging

The features adds an SD-WAN daemon function to keep a short, 10 minute history of SLA that can be viewed in the CLI.

Performance SLA results related to interface selection, session failover, and other information, can be logged. These logs can then be used for long-term monitoring of traffic issues at remote sites, and for reports and views in FortiAnalyzer.

The time intervals that Performance SLA fail and pass logs are generated in can be configured.

To configure the fail and pass logs' generation time interval:

```
config system virtual-wan-link
    config health-check
        edit "ping"
            set sla-fail-log-period 30
```

```

        set sla-pass-log-period 60
    next
end
end

```

To view the 10 minute Performance SLA link status history:

```

FGT_A (root) # diagnose sys virtual-wan-link sla-log ping 1
Timestamp: Thu Feb 28 10:58:24 2019, vdom root, health-check ping, interface: R150, status:
up, latency: 0.000, jitter: 0.000, packet loss: 0.000%.
Timestamp: Thu Feb 28 10:58:24 2019, vdom root, health-check ping, interface: R150, status:
up, latency: 0.097, jitter: 0.000, packet loss: 0.000%.
Timestamp: Thu Feb 28 10:58:25 2019, vdom root, health-check ping, interface: R150, status:
up, latency: 0.058, jitter: 0.040, packet loss: 0.000%.
Timestamp: Thu Feb 28 10:58:25 2019, vdom root, health-check ping, interface: R150, status:
up, latency: 0.044, jitter: 0.026, packet loss: 0.000%.
... ..

```

SLA pass logs

The FortiGate generates Performance SLA logs at the specified pass log interval (sla-pass-log-period) when SLA passes.

```

3: date=2019-02-28 time=11:53:26 logid="0100022925" type="event" subtype="system"
level="information" vd="root" eventtime=1551383604 logdesc="Link monitor SLA information"
name="ping" interface="R160" status="up" msg="Latency: 0.013, jitter: 0.001, packet loss:
0.000%, inbandwidth: 0Mbps, outbandwidth: 0Mbps, bibandwidth: 0Mbps, sla_map: 0x1"
7: date=2019-02-28 time=11:52:26 logid="0100022925" type="event" subtype="system"
level="information" vd="root" eventtime=1551383545 logdesc="Link monitor SLA information"
name="ping" interface="R160" status="up" msg="Latency: 0.013, jitter: 0.002, packet loss:
0.000%, inbandwidth: 0Mbps, outbandwidth: 0Mbps, bibandwidth: 0Mbps, sla_map: 0x1"

```

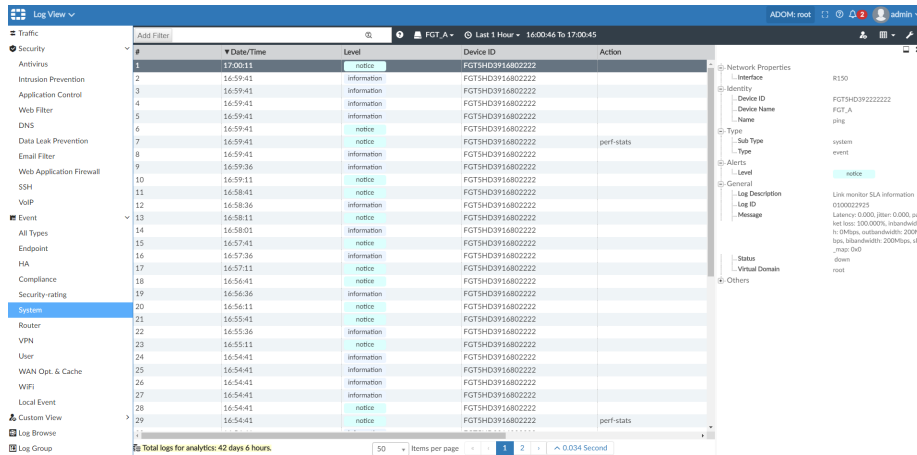
In the FortiAnalyzer GUI:

#	Date/Time	Level	Device ID	Action
1	17:00:11	notice	FGTSHD3916802222	
2	16:59:41	information	FGTSHD3916802222	
3	16:59:41	information	FGTSHD3916802222	
4	16:59:41	information	FGTSHD3916802222	
5	16:59:41	information	FGTSHD3916802222	
6	16:59:41	notice	FGTSHD3916802222	
7	16:59:41	notice	FGTSHD3916802222	perf-stats
8	16:59:41	information	FGTSHD3916802222	
9	16:59:36	information	FGTSHD3916802222	
10	16:59:11	notice	FGTSHD3916802222	
11	16:58:41	notice	FGTSHD3916802222	
12	16:58:36	information	FGTSHD3916802222	
13	16:58:11	notice	FGTSHD3916802222	
14	16:58:01	information	FGTSHD3916802222	
15	16:57:41	notice	FGTSHD3916802222	
16	16:57:36	information	FGTSHD3916802222	
17	16:57:11	notice	FGTSHD3916802222	
18	16:56:41	notice	FGTSHD3916802222	
19	16:56:36	information	FGTSHD3916802222	
20	16:56:11	notice	FGTSHD3916802222	
21	16:55:41	notice	FGTSHD3916802222	
22	16:55:36	information	FGTSHD3916802222	
23	16:55:11	notice	FGTSHD3916802222	
24	16:54:41	information	FGTSHD3916802222	
25	16:54:41	information	FGTSHD3916802222	
26	16:54:41	information	FGTSHD3916802222	
27	16:54:41	information	FGTSHD3916802222	
28	16:54:41	notice	FGTSHD3916802222	
29	16:54:41	notice	FGTSHD3916802222	perf-stats

SLA fail logs

The FortiGate generates Performance SLA logs at the specified fail log interval (sla-fail-log-period) when SLA fails.


```
6: date=2019-02-28 time=11:52:32 logid="0100022925" type="event" subtype="system"
level="notice" vd="root" eventtime=1551383552 logdesc="Link monitor SLA information"
name="ping" interface="R150" status="down" msg="Latency: 0.000, jitter: 0.000, packet loss:
100.000%, inbandwidth: 0Mbps, outbandwidth: 200Mbps, bibandwidth: 200Mbps, sla_map: 0x0"
8: date=2019-02-28 time=11:52:02 logid="0100022925" type="event" subtype="system"
level="notice" vd="root" eventtime=1551383522 logdesc="Link monitor SLA information"
name="ping" interface="R150" status="down" msg="Latency: 0.000, jitter: 0.000, packet loss:
100.000%, inbandwidth: 0Mbps, outbandwidth: 200Mbps, bibandwidth: 200Mbps, sla_map: 0x0"
```



SLA monitoring using the REST API

SLA log information and interface SLA information can be monitored using the REST API. This feature is also be used by FortiManager as part of its detailed SLA monitoring and drill-down features.

Interface log command example:

```
https://172.172.172.9/api/v2/monitor/virtual-wan/interface-log
{
  "http_method": "GET",
  "results": [
    {
      "interface": "port13",
      "logs": [
        {
          "timestamp": 1547087168,
          "tx_bandwidth": 3447,
          "rx_bandwidth": 3457,
          "bi_bandwidth": 6904,
          "tx_bytes": 748875,
          "rx_bytes": 708799,
          "egress_queue": [
          ]
        },
        {
          "timestamp": 1547087178,
          "tx_bandwidth": 3364,
          "rx_bandwidth": 3400,
          "bi_bandwidth": 6764,

```

```

        "tx_bytes":753789,
        "rx_bytes":712835,
        "egress_queue":[
    ]
},
....
....

```

SLA log command example:

<https://172.172.172.9/api/v2/monitor/virtual-wan/sla-log>

```

{
  "http_method":"GET",
  "results":[
    {
      "name":"ping",
      "interface":"port13",
      "logs":[
        {
          "timestamp":1547087204,
          "link":"up",
          "latency":0.686433,
          "jitter":0.063400,
          "packetloss":0.000000
        },
        {
          "timestamp":1547087205,
          "link":"up",
          "latency":0.688433,
          "jitter":0.063133,
          "packetloss":0.000000
        },
        {
          "timestamp":1547087206,
          "link":"up",
          "latency":0.688300,
          "jitter":0.065267,
          "packetloss":0.000000
        }
      ],
    },
    ....
    ....
  ]
}

```

CLI diagnose commands:

```

# diagnose sys virtual-wan-link sla-log ping 1
Timestamp: Wed Jan 9 18:35:11 2019, vdom root, health-check ping, interface: port13,
status: up, latency: 0.698, jitter: 0.073, packet loss: 0.000%.
Timestamp: Wed Jan 9 18:35:12 2019, vdom root, health-check ping, interface: port13,
status: up, latency: 0.704, jitter: 0.073, packet loss: 0.000%.
Timestamp: Wed Jan 9 18:35:13 2019, vdom root, health-check ping, interface: port13,
status: up, latency: 0.709, jitter: 0.073, packet loss: 0.000%.
Timestamp: Wed Jan 9 18:35:14 2019, vdom root, health-check ping, interface: port13,
status: up, latency: 0.707, jitter: 0.066, packet loss: 0.000%.
Timestamp: Wed Jan 9 18:35:15 2019, vdom root, health-check ping, interface: port13,
status: up, latency: 0.710, jitter: 0.061, packet loss: 0.000%.
Timestamp: Wed Jan 9 18:35:16 2019, vdom root, health-check ping, interface: port13,

```

```
status: up, latency: 0.707, jitter: 0.055, packet loss: 0.000%.
  Timestamp: Wed Jan 9 18:35:17 2019, vdom root, health-check ping, interface: port13,
status: up, latency: 0.703, jitter: 0.055, packet loss: 0.000%.

# diagnose sys virtual-wan-link intf-sla-log port13
  Timestamp: Wed Jan 9 18:33:49 2019, used inbandwidth: 3208bps, used outbandwidth:
3453bps, used bibandwidth: 6661bps, tx bytes: 947234bytes, rx bytes: 898622bytes.
  Timestamp: Wed Jan 9 18:33:59 2019, used inbandwidth: 3317bps, used outbandwidth:
3450bps, used bibandwidth: 6767bps, tx bytes: 951284bytes, rx bytes: 902937bytes.
  Timestamp: Wed Jan 9 18:34:09 2019, used inbandwidth: 3302bps, used outbandwidth:
3389bps, used bibandwidth: 6691bps, tx bytes: 956268bytes, rx bytes: 907114bytes.
  Timestamp: Wed Jan 9 18:34:19 2019, used inbandwidth: 3279bps, used outbandwidth:
3352bps, used bibandwidth: 6631bps, tx bytes: 958920bytes, rx bytes: 910793bytes.
  Timestamp: Wed Jan 9 18:34:29 2019, used inbandwidth: 3233bps, used outbandwidth:
3371bps, used bibandwidth: 6604bps, tx bytes: 964374bytes, rx bytes: 914854bytes.
  Timestamp: Wed Jan 9 18:34:39 2019, used inbandwidth: 3235bps, used outbandwidth:
3362bps, used bibandwidth: 6597bps, tx bytes: 968250bytes, rx bytes: 918846bytes.
  Timestamp: Wed Jan 9 18:34:49 2019, used inbandwidth: 3165bps, used outbandwidth:
3362bps, used bibandwidth: 6527bps, tx bytes: 972298bytes, rx bytes: 922724bytes.
  Timestamp: Wed Jan 9 18:34:59 2019, used inbandwidth: 3184bps, used outbandwidth:
3362bps, used bibandwidth: 6546bps, tx bytes: 977282bytes, rx bytes: 927019bytes.
```

SD-WAN bandwidth monitoring service

The bandwidth measuring tool is used to detect true upload and download speeds. Bandwidth tests can be run on demand or automated using a script to measure upload and download speeds up to 1 Gbps of throughput. This can be useful when configuring SD-WAN SLA and rules to balance SD-WAN traffic.

The speed test tool requires a valid SD-WAN Bandwidth Monitoring Service license.

The speed test tool is compatible with iperf3.6 with SSL support. It can test the upload bandwidth to the FortiGate Cloud speed test service. It can initiate the server connection and send download requests to the server. The tool can be run up to 10 times a day .

FortiGate downloads the speed test server list. The list expires after 24 hours. One of the speed test servers is selected, based on user input. The speed test runs, testing upload and download speeds. The test results are shown in the command terminal.

To download the speed test server list:

```
# execute speed-test-server download
Download completed.
```

To check the speed test server list:

```
# execute speed-test-server list
AWS_West valid
  Host: 34.210.67.183 5204 fortinet
  Host: 34.210.67.183 5205 fortinet
  Host: 34.210.67.183 5206 fortinet
  Host: 34.210.67.183 5207 fortinet
Google_West valid
  Host: 35.197.55.210 5204 fortinet
  Host: 35.197.55.210 5205 fortinet
```

```
Host: 35.197.55.210 5206 fortinet
Host: 35.197.55.210 5207 fortinet
Host: 35.230.2.124 5204 fortinet
Host: 35.230.2.124 5205 fortinet
Host: 35.230.2.124 5206 fortinet
Host: 35.230.2.124 5207 fortinet
Host: 35.197.18.234 5204 fortinet
Host: 35.197.18.234 5205 fortinet
Host: 35.197.18.234 5206 fortinet
Host: 35.197.18.234 5207 fortinet
```

To run the speed test:

You can run the speed test without specifying a server. The system will automatically choose one server from the list and run the speed test.

```
# execute speed-test auto
The license is valid to run speed test.
Speed test quota for 2/1 is 9
current vdom=root
Run in uploading mode.
Connecting to host 35.230.2.124, port 5206
[ 16] local 172.16.78.185 port 2475 connected to 35.230.2.124 port 5206
[ ID] Interval Transfer Bitrate Retr Cwnd
[ 16] 0.00-1.01 sec 11.0 MBytes 91.4 Mbits/sec 0 486 KBytes
[ 16] 1.01-2.00 sec 11.6 MBytes 98.4 Mbits/sec 0 790 KBytes
[ 16] 2.00-3.01 sec 11.0 MBytes 91.6 Mbits/sec 15 543 KBytes
[ 16] 3.01-4.01 sec 11.2 MBytes 94.2 Mbits/sec 1 421 KBytes
[ 16] 4.01-5.01 sec 11.2 MBytes 93.5 Mbits/sec 0 461 KBytes
- - - - -
[ ID] Interval Transfer Bitrate Retr
[ 16] 0.00-5.01 sec 56.1 MBytes 93.8 Mbits/sec 16 sender
[ 16] 0.00-5.06 sec 55.8 MBytes 92.6 Mbits/sec receiver

speed test Done.
Run in reverse downloading mode!
Connecting to host 35.230.2.124, port 5206
Reverse mode, remote host 35.230.2.124 is sending
[ 16] local 172.16.78.185 port 2477 connected to 35.230.2.124 port 5206
[ ID] Interval Transfer Bitrate
[ 16] 0.00-1.00 sec 10.9 MBytes 91.4 Mbits/sec
[ 16] 1.00-2.00 sec 11.2 MBytes 93.9 Mbits/sec
[ 16] 2.00-3.00 sec 11.2 MBytes 94.0 Mbits/sec
[ 16] 3.00-4.00 sec 11.2 MBytes 93.9 Mbits/sec
[ 16] 4.00-5.00 sec 10.9 MBytes 91.1 Mbits/sec
- - - - -
[ ID] Interval Transfer Bitrate Retr
[ 16] 0.00-5.03 sec 57.5 MBytes 95.9 Mbits/sec 40 sender
[ 16] 0.00-5.00 sec 55.4 MBytes 92.9 Mbits/sec receiver

speed test Done
```

To run the speed test on a server farm or data center:

```
# execute speed-test auto AWS_West
The license is valid to run speed test.
```

```
Speed test quota for 2/1 is 8
current vdom=root
Run in uploading mode.
Connecting to host 34.210.67.183, port 5205
```

To run the speed test on a local interface when there are multiple valid routes:

```
# execute speed-test port1 Google_West
The license is valid to run speed test.
Speed test quota for 2/1 is 6
bind to local ip 172.16.78.202
current vdom=root
Specified interface port1 does not comply with default outgoing interface port2 in routing
table!
Force to use the specified interface!
Run in uploading mode.
Connecting to host 35.197.18.234, port 5205
[ 11] local 172.16.78.202 port 20852 connected to 35.197.18.234 port 5205
[ ID] Interval Transfer Bitrate Retr Cwnd
[ 11] 0.00-1.01 sec 10.7 MBytes 89.0 Mbits/sec 0 392 KBytes
[ 11] 1.01-2.01 sec 10.5 MBytes 88.5 Mbits/sec 1 379 KBytes
[ 11] 2.01-3.01 sec 11.3 MBytes 94.5 Mbits/sec 0 437 KBytes
[ 11] 3.01-4.01 sec 11.2 MBytes 94.3 Mbits/sec 0 478 KBytes
[ 11] 4.01-5.00 sec 11.3 MBytes 95.2 Mbits/sec 0 503 KBytes
- - - - -
[ ID] Interval Transfer Bitrate Retr
[ 11] 0.00-5.00 sec 55.1 MBytes 92.3 Mbits/sec 1 sender
[ 11] 0.00-5.04 sec 54.5 MBytes 90.7 Mbits/sec receiver

speed test Done.
Run in reverse downloading mode!
Connecting to host 35.197.18.234, port 5205
Reverse mode, remote host 35.197.18.234 is sending
[ 11] local 172.16.78.202 port 20853 connected to 35.197.18.234 port 5205
[ ID] Interval Transfer Bitrate
[ 11] 0.00-1.00 sec 10.9 MBytes 91.1 Mbits/sec
[ 11] 1.00-2.00 sec 11.2 MBytes 94.0 Mbits/sec
[ 11] 2.00-3.00 sec 11.2 MBytes 94.0 Mbits/sec
[ 11] 3.00-4.00 sec 11.2 MBytes 94.0 Mbits/sec
[ 11] 4.00-5.00 sec 11.2 MBytes 94.0 Mbits/sec
- - - - -
[ ID] Interval Transfer Bitrate Retr
[ 11] 0.00-5.03 sec 57.4 MBytes 95.8 Mbits/sec 33 sender
[ 11] 0.00-5.00 sec 55.7 MBytes 93.4 Mbits/sec receiver

speed test Done.
```

To add a script to run a speed test automatically once every 24 hours:

```
config system auto-script
    edit "speedtest"
        set interval 86400
        set repeat 0
        set start auto
        set script "
execute speed-test-server download
```

```
execute speed-test"  
  next  
end
```

To view the results of the speed test script:

```
execute auto-script result speedtest
```

System

This topic contains information about FortiGate administration and system configuration that you can do after installing the FortiGate in your network.

Basic system settings

Administrators

By default, FortiGate has an administrator account with the username *admin* and no password. See [Administrators on page 619](#) for more information.

Administrator profiles

An administrator profile defines what the administrator can see and do on the FortiGate. See [Administrator profiles on page 619](#) for more information.

Password policy

Set up a password policy to enforce password criteria and change frequency. See [Password policy on page 624](#) for more information.

Interfaces

Physical and virtual interface allow traffic to flow between internal networks, and between the internet and internal networks. See [Interfaces on page 315](#) for more information.

Advanced system settings

SNMP

The simple network management protocol (SNMP) allows you to monitor hardware on your network. See [SNMP on page 707](#) for more information.

DHCP server

You can configure one or more DHCP servers on any FortiGate interface. See [DHCP server on page 400](#) for more information.

VDOM

You can use virtual domains (VDOMs) to divide a FortiGate into multiple virtual devices that function independently. See [Virtual Domains on page 650](#) for more information.

High availability

You can configure multiple FortiGate devices, including private and public cloud VMs, in HA mode. See [High Availability on page 671](#) for more information.

Certificates

You can manage certificates on the FortiGate. See [Certificates on page 733](#) for more information.

Operating modes

A FortiGate or VDOM (in multi-vdom mode) can operate in either NAT/Route mode or Transparent mode.

NAT/Route mode

The FortiGate or VDOM is installed as a gateway between two networks, such as a private network and the internet. This allows the FortiGate to hide the IP addresses on the private network using NAT. NAT/Route mode can also be used when several ISPs are used for redundant internet connections.

By default, new VDOMs are set to NAT/Route operation mode.

See [Configure VDOM-A on page 658](#) for more information.

Transparent mode

The FortiGate or VDOM is installed between the internal network and the router. The FortiGate does not change any IP addresses, and only applies security scanning to traffic. When you add a FortiGate that is in transparent mode to a network, it only needs to be provided with a management IP address.

Transparent mode is primarily used when increased network protection is needed without changing the network configuration.

See [Configure VDOM-A on page 667](#) for more information.

To change the operating mode of a FortiGate or VDOM:

```
config system settings
    set opmode {nat | transparent}
end
```


Administrators

By default, FortiGate has an administrator account with the username *admin* and no password. To prevent unauthorized access to the FortiGate, this account must be protected with a password. Additional administrators can be added for various functions, each with a unique username, password, and set of access privileges.

The following topics provide information about administrators:

- [Administrator profiles on page 619](#)
- [Add a local administrator on page 621](#)
- [Remote authentication for administrators on page 621](#)
- [Password policy on page 624](#)
- [Associating a FortiToken to an administrator account on page 625](#)

Administrator profiles

Administrator profiles define what the administrator can do when logged into the FortiGate. When you set up an administrator account, you also assign an administrator profile which dictates what the administrator sees. Depending on the nature of the administrator's work, access level or seniority, you can allow them to view and configure as much or as little as is required.

By default, the FortiGate has an *admin* administrator account that uses the *super_admin* profile.

Super_admin profile

This profile has access to all components of FortiOS, including the ability to add and remove other system administrators. For certain administrative functions, such as backing up and restoring the configuration, *super_admin* access is required. To ensure that there is always a method to administer the FortiGate, the *super_admin* profile can't be deleted or modified.



Lower level administrator profiles can't backup or restore the FortiOS configuration.

The *super_admin* profile is used by the default *admin* account. It is recommended that you add a password and rename this account once you have set up your FortiGate. In order to rename the default account, a second *admin* account is required.

Creating customized profiles

To create a profile in the GUI:

1. Go to *System > Admin Profiles*.
2. Select *Create New*.
3. Configure the following settings:
 - Name.
 - Access permissions.

- Override idle timeout.

4. Select *OK*.

To create a profile in the CLI:

```
config system accprofile
  edit "sample"
    set secfabgrp read-write
    set ftviewgrp read-write
    set authgrp read-write
    set sysgrp read-write
    set netgrp read-write
    set loggrp read-write
    set fwgrp read-write
    set vpngrp read-write
    set utmgrp read-write
    set wanoptgrp read-write
    set wifi read-write
  next
end
```

Edit profiles

To edit a profile in the GUI:

1. Go to *System > Admin Profiles*.
2. Choose the profile to be edited and select *Edit*.
3. Select *OK* to save any changes made.

To edit a profile in the CLI:

```
config system accprofile
  edit "sample"
    set secfabgrp read
  next
end
```

Delete profiles

To delete a profile in the GUI:

1. Go to *System > Admin Profiles*.
2. Choose the profile to be deleted and select *Delete*.
3. Select *OK*.

To delete a profile in the CLI:

```
config system accprofile
  delete "sample"
end
```

Add a local administrator

By default, FortiGate has one super admin named `admin`. You can create more administrator accounts with different privileges.

To create an administrator account in the GUI:

1. Go to *System > Administrators*.
2. Select *Create New > Administrator*.
3. Specify the *Username*.



Do not use the characters `< > () # " '` in the administrator username.
Using these characters in an administrator username might have a cross site scripting (XSS) vulnerability.

4. Set *Type* to *Local User*.
5. Set the password and other fields.
6. Click *OK*.

To create an administrator account in the CLI:

```
config system admin
  edit <admin_name>
    set accprofile <profile_name>
    set vdom <vdom_name>
    set password <password for this admin>
  next
end
```

Remote authentication for administrators

Administrators can use remote authentication, such as LDAP, to connect to the FortiGate.

Setting up remote authentication for administrators includes the following steps:

1. [Configuring the LDAP server on page 621](#)
2. [Adding the LDAP server to a user group on page 622](#)
3. [Configuring the administrator account on page 622](#)

Configuring the LDAP server

To configure the LDAP server in the GUI:

1. Go to *User & Device > LDAP Servers* and click *Create New*.
2. Enter the server *Name* and *Server IP/Name*.
3. Enter the *Common Name Identifier* and *Distinguished Name*.
4. Set the *Bind Type* to *Regular* and enter the *Username* and *Password*.
5. Click *OK*.

To configure the LDAP server in the CLI:

```
config user ldap
  edit <name>
    set server <server_ip>
    set cnid "cn"
    set dn "dc=XYZ,dc=fortinet,dc=COM"
    set type regular
    set username "cn=Administrator,dc=XYA, dc=COM"
    set password <password>
  next
end
```

Adding the LDAP server to a user group

After configuring the LDAP server, create a user group that includes that LDAP server.

To create a user group in the GUI:

1. Go to *User & Device > User Groups* and click *Create New*.
2. Enter a *Name* for the group.
3. In the *Remote groups* section, select *Create New*.
4. Select the *Remote Server* from the dropdown list.
5. Click *OK*.

To create a user group in the CLI:

```
config user group
  edit <name>
    set member <ldap_server_name>
  next
end
```

Configuring the administrator account

After configuring the LDAP server and adding it to a user group, create a new administrator. For this administrator, instead of entering a password, use the new user group for authentication.

To create an administrator in the GUI:

1. Go to *System > Administrators* and click *Create New > Administrator*.
2. Specify the *Username*.
3. Set *Type* to *Match all users in a remote server group*.
4. In *Remote User Group*, select the user group you created.
5. Select an *Administrator Profile*.
6. Click *OK*.

To create an administrator in the CLI:

```
config system admin
  edit <name>
    set remote-auth enable
    set accprofile super_admin
    set wildcard enable
    set remote-group <ldap_group_name>
  next
end
```



The *Match all users in a remote server group* option acts as a wildcard for matching any users against the remote server group. The *Match a user on a remote server group* option only matches the username defined to match against the remote server group, which is the equivalent of using `set wildcard disable`.

Other methods of administrator authentication

Administrator accounts can use different methods for authentication, including RADIUS, TACACS+, and PKI.

RADIUS authentication for administrators

To use a RADIUS server to authenticate administrators, you must:

1. Configure the FortiGate to access the RADIUS server.
2. Create the RADIUS user group.
3. Configure an administrator to authenticate with a RADIUS server.

TACACS+ authentication for administrators

To use a TACACS+ server to authenticate administrators, you must:

1. Configure the FortiGate to access the TACACS+ server.
2. Create a TACACS+ user group.
3. Configure an administrator to authenticate with a TACACS+ server.

PKI certificate authentication for administrators

To use PKI authentication for an administrator, you must:

1. Configure a PKI user.
2. Create a PKI user group.
3. Configure an administrator to authenticate with a PKI certificate.

Restricting logins from local administrator accounts when remote servers are available

There is an optional setting that restricts logins from local administrator accounts when remote servers are available. This is disabled by default, but can be enabled globally. This option only works when all configured remote servers are down.

To restrict local administrator authentication when a remote authentication server is running:

```
config system global
    set admin-restrict-local enable
end
```

Password policy

Brute force password software can launch more than just dictionary attacks. It can discover common passwords where a letter is replaced by a number. For example, if `p4ssw0rd` is used as a password, it can be cracked.

Using secure passwords is vital for preventing unauthorized access to your FortiGate. When changing the password, consider the following to ensure better security:

- Do not use passwords that are obvious, such as the company name, administrator names, or other obvious words or phrases.
- Use numbers in place of letters, for example: `passw0rd`.
- Administrator passwords can be up to 64 characters.
- Include a mixture of numbers, symbols, and upper and lower case letters.
- Use multiple words together, or possibly even a sentence, for example: `correcthorsebatterystaple`.
- Use a password generator.
- Change the password regularly and always make the new password unique and not a variation of the existing password. For example, do not change from `password` to `password1`.
- Make note of the password and store it in a safe place away from the management computer, in case you forget it; or ensure at least two people know the password in the event one person becomes unavailable. Alternatively, have two different admin logins.

FortiGate allows you to create a password policy for administrators and IPsec pre-shared keys. With this policy, you can enforce regular changes and specific criteria for a password policy, including:

- Minimum length between 8 and 64 characters.
- If the password must contain uppercase (A, B, C) and/or lowercase (a, b, c) characters.
- If the password must contain numbers (1, 2, 3).
- If the password must contain special or non-alphanumeric characters (!, @, #, \$, %, ^, &, *, (, and)).
- Where the password applies (admin or IPsec or both).
- The duration of the password before a new one must be specified.

If you add a password policy or change the requirements on an existing policy, the next time that administrator logs into the FortiGate, the administrator is prompted to update the password to meet the new requirements before proceeding to log in.

For information about setting passwords, see [Default administrator password on page 633](#).

To create a system password policy the GUI:

1. Go to *System > Settings*.
2. In the *Password Policy* section, change the *Password scope* to *Admin*, *IPsec*, or *Both*.
3. Configure the password policy options.
4. Click *Apply*.

To create a system password policy the CLI:

```
config system password-policy
  set status {enable | disable}
  set apply-to {admin-password | ipsec-preshared-key}
  set minimum-length <8-128>
  set min-lower-case-letter <0-128>
  set min-upper-case-letter <0-128>
  set min-non-alphanumeric <0-128>
  set min-number <0-128>
  set change-4-characters {enable | disable}
  set expire-status {enable | disable}
  set expire-day <1-999>
  set reuse-password {enable | disable}
end
```

Associating a FortiToken to an administrator account

You can also associate FortiTokens with administrator accounts.

To associate a FortiToken to an administrator account using the GUI:

1. Ensure that you have successfully added your FortiToken serial number to FortiOS and that its status is Available.
2. Go to *System > Administrators*. Edit the admin account. This example assumes that the account is fully configured except for two-factor authentication.
3. In the *Email Address* field, enter the administrator's email address.
4. Enable *Two-factor Authentication*.
5. From the *Token* dropdown list, select the desired FortiToken serial number.
6. Click *OK*.



For a mobile token, click *Send Activation Code* to send the activation code to the configured email address. The admin uses this code to activate their mobile token. You must have configured an email service in *System > Settings* to send the activation code.

To associate a FortiToken to an administrator account using the CLI:

```
config system admin
  edit <username>
    set password "myPassword"
    set two-factor fortitoken
    set fortitoken <serial_number>
    set email-to "username@example.com"
  next
end
```

The `fortitoken` keyword is not visible until you select `fortitoken` for the `two-factor` option.



Before you can use a new FortiToken, you may need to synchronize it due to clock drift.

Firmware

Fortinet periodically updates the FortiGate firmware to include new features and resolve important issues. After you have registered your FortiGate unit, firmware updates can be downloaded from the [Fortinet Customer Service & Support](#) website.



Always back up the current configuration before installing new firmware. See [Configuration backups on page 62](#).

Before you install any new firmware, follow the below steps:

1. Review the [Release Notes](#) for a new firmware release.
2. Review the [Supported Upgrade Paths](#).
3. Download a copy of the currently installed firmware, in case you need to revert to it. See [Downloading a firmware image on page 626](#) and [Downgrading to a previous firmware version on page 629](#) for details.
4. Have a plan in place in case there is a critical failure, such as the FortiGate not coming back online after the update. This could include having console access to the device ([Connecting to the CLI on page 23](#)), ensuring that you TFTP server is working ([Installing firmware from system reboot on page 630](#)), and preparing a USB drive ([Restoring from a USB drive on page 631](#)).
5. Backup the current configuration, including local certificates. See [Configuration backups on page 62](#) for details.
6. Test the new firmware until you are satisfied that it applies to your configuration. See [Testing a firmware version on page 627](#) and [Controlled upgrade on page 632](#) for details.

Installing new firmware without reviewing release notes or testing the firmware may result in changes to settings and unexpected issues.



Only FortiGate admin users and administrators whose access profiles contain system read and write privileges can change the FortiGate firmware.

Downloading a firmware image

Firmware images for all FortiGate units are available on the [Fortinet Customer Service & Support](#) website.

To download firmware:

1. Log into the support site with your user name and password.
2. Go to *Download > Firmware Images*.
A list of Release Notes is shown. If you have not already done so, download and review the Release Notes for the firmware version that you are upgrading your FortiGate unit to.
3. Select the *Download* tab.
4. Navigate to the folder for the firmware version that you are upgrading to.
5. Find your device model from the list. FortiWiFi devices have file names that start with *FWF*.
6. Click *HTTPS* in the far right column to download the firmware image to your computer.



Firmware can also be downloaded using FTP, but as FTP is not an encrypted file transferring protocol, HTTPS downloading is recommended.

Testing a firmware version

The integrity of firmware images downloaded from Fortinet's support portal can be verified using a file checksum. A file checksum that does not match the expected value indicates a corrupt file. The corruption could be caused by errors in transfer or by file modification. A list of expected checksum values for each build of released code is available on Fortinet's support portal.

Image integrity is also verified when the FortiGate is booting up. This integrity check is done through a cyclic redundancy check (CRC). If the CRC fails, the FortiGate unit will encounter an error during the boot process.

Firmware images are signed and the signature is attached to the code as it is built. When upgrading an image, the running OS will generate a signature and compare it with the signature attached to the image. If the signatures do not match, the new OS will not load.

Testing before installation

FortiOS lets you test a new firmware image by installing the firmware image from a system reboot and saving it to system memory. After completing this procedure, the FortiGate unit operates using the new firmware image with the current configuration. The new firmware image is not permanently installed. The next time the FortiGate unit restarts, it operates with the originally installed firmware image using the current configuration. If the new firmware image operates successfully, you can install it permanently using the procedure explained in [Upgrading the firmware](#).

For this procedure, you must install a TFTP server that you can connect to from the FortiGate internal interface. The TFTP server should be on the same subnet as the internal interface.

To test the new firmware version:

1. Connect to the CLI using an RJ-45 to USB (or DB-9) or null modem cable.
2. Ensure that the TFTP server is running.
3. Copy the new firmware image file to the root directory on the TFTP server.
4. Ensure that the FortiGate unit can connect to the TFTP server using the `execute ping` command.
5. Restart the FortiGate unit: `execute reboot`. The following message is shown:

```
This operation will reboot the system!
Do you want to continue? (y/n)
```
6. Type `y`. As the FortiGate unit starts, a series of system startup messages appears.
7. When the following messages appears:

```
Press any key to display configuration menu.....
```

Immediately press any key to interrupt the system startup.

You have only three seconds to press any key. If you do not press a key during this time, the FortiGate will reboot, and you will have to log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default
[C]: Configuration and information
```

[Q]: Quit menu and continue to boot with default firmware.

[H]: Display this list of options.

Enter G, F, Q, or H:

8. Type **G** to get the new firmware image from the TFTP server. The following message appears: Enter TFTP server address [192.168.1.168]:
9. Type the address of the TFTP server, then press **Enter**. The following message appears: Enter Local Address [192.168.1.188]:
10. Type the IP address of the FortiGate unit to connect to the TFTP server.



The IP address must be on the same network as the TFTP server.
Make sure that you do not enter the IP address of another device on this network.

The following message appears:

Enter File Name [image.out]:

11. Enter the firmware image file name then press **Enter**. The TFTP server uploads the firmware image file to the FortiGate unit and the following message appears:
Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]
12. Type **R**. The FortiGate image is installed to system memory and the FortiGate unit starts running the new firmware image, but with its current configuration.

Test the new firmware image as required. When done testing, reboot the FortiGate unit, and the it will resume using the firmware that was running before you installed the test firmware.

Upgrading the firmware

Installing a new firmware image replaces the current antivirus and attack definitions, along with the definitions included with the firmware release that is being installing. After you install new firmware, make sure that the antivirus and attack definitions are up to date.



Back up your configuration before making any firmware changes.

To upgrade the firmware in the GUI:

1. Log into the FortiGate GUI as the admin administrative user.
2. Go to *System > Firmware*.
3. Under *Upload Firmware*, click *Browse* and locate the previously downloaded firmware image file (see [Downloading a firmware image on page 626](#)).
4. Click *Backup config and upgrade*.
The FortiGate unit backs up the current configuration to the management computer, uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.

To upgrade the firmware in the CLI:

1. Make sure that the TFTP server is running.
2. Copy the new firmware image file to the root directory of the TFTP server.

3. Log into the CLI.
4. Ping the TFTP server to ensure that the FortiGate can connect to it:

```
execute ping <tftp_ipv4>
```
5. Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:

```
execute restore image tftp <filename> <tftp_ipv4>
```

The FortiGate unit responds with the message:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```
6. Type `y`. The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.
7. Reconnect to the CLI.
8. Update the antivirus and attack definitions:

```
execute update-now
```

Downgrading to a previous firmware version



Downgrading the firmware is not recommended.

This procedure downgrades the FortiGate to a previous firmware version. The backup configuration might not be able to be restored after downgrading.

To downgrade to a previous firmware version in the GUI:

1. Log into the FortiGate GUI as the admin administrative user.
 2. Go to *System > Firmware*.
 3. Under *Upload Firmware*, click *Browse* and locate the previously downloaded firmware image file (see [Downloading a firmware image on page 626](#)).
 4. Click *Confirm version downgrade*.
 5. Click *Backup config and downgrade*.
- The FortiGate unit backs up the current configuration to the management computer, uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.

To downgrade to a previous firmware version in the CLI:

1. Make sure that the TFTP server is running.
2. Copy the new firmware image file to the root directory of the TFTP server.
3. Log into the CLI.
4. Ping the TFTP server to ensure that the FortiGate can connect to it:

```
execute ping <tftp_ipv4>
```
5. Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:

```
execute restore image tftp <filename> <tftp_ipv4>
```

The FortiGate unit responds with the message:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```
6. Type `y`. The FortiGate unit uploads the firmware image file, then a message similar to the following is shown:

```
Get image from tftp server OK.
```

```

Check image OK.
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)

```

7. Type `y`. The FortiGate unit downgrades to the old firmware version and restarts. This process takes a few minutes.
8. Reconnect to the CLI.
9. Update the antivirus and attack definitions:

```
execute update-now
```

Installing firmware from system reboot

In the event that the firmware upgrade does not load properly and the FortiGate unit will not boot, or continuously reboots, it is best to perform a fresh install of the firmware from a reboot using the CLI. If configured, the firmware can also be automatically installed from a USB drive; see [Restoring from a USB drive on page 631](#) for details.

This procedure installs a firmware image and resets the FortiGate unit to factory default settings. You can use this procedure to upgrade to a new firmware version, revert to an older firmware version, or re-install the current firmware.

To use this procedure, you must connect to the CLI using the FortiGate console port and a RJ-45 to USB (or DB-9), or null modem cable. You must also install a TFTP server that you can connect to from the FortiGate internal interface. The TFTP server should be on the same subnet as the internal interface.

Before beginning this procedure, ensure that you backup the FortiGate unit configuration. See [Configuration backups on page 62](#) for details. If you are reverting to a previous FortiOS version, you might not be able to restore the previous configuration from the backup configuration file.

Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date.

To install firmware from a system reboot:

1. Connect to the CLI using the RJ-45 to USB (or DB-9) or null modem cable.
2. Ensure that the TFTP server is running.
3. Copy the new firmware image file to the root directory of the TFTP server.
4. Ensure that the FortiGate unit can connect to the TFTP server using the `execute ping` command.
5. Restart the FortiGate unit: `execute reboot`. The following message is shown:

```

This operation will reboot the system!
Do you want to continue? (y/n)

```

6. Type `y`. As the FortiGate unit starts, a series of system startup messages appears.
7. When the following messages appears:

```
Press any key to display configuration menu.....
```

Immediately press any key to interrupt the system startup.

You have only three seconds to press any key. If you do not press a key during this time, the FortiGate will reboot, and you will have to log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following messages appears:

```

[C]: Configure TFTP parameters.
[R]: Review TFTP parameters.
[T]: Initiate TFTP firmware transfer.
[F]: Format boot device.
[I]: System information.

```

[B]: Boot with backup firmware and set as default.
 [Q]: Quit menu and continue to boot.
 [H]: Display this list of options.

Enter C,R,T,F,I,B,Q, or H:

8. If necessary, type C to configure the TFTP parameters, then type Q to return to the previous menu:

[P]: Set firmware download port.
 [D]: Set DHCP mode.
 [I]: Set local IP address.
 [S]: Set local subnet mask.
 [G]: Set local gateway.
 [V]: Set local VLAN ID.
 [T]: Set remote TFTP server IP address.
 [F]: Set firmware file name.
 [E]: Reset TFTP parameters to factory defaults.
 [R]: Review TFTP parameters.
 [N]: Diagnose networking (ping).
 [Q]: Quit this menu.
 [H]: Display this list of options.

Enter P,D,I,S,G,V,T,F,E,R,N,Q, or H:



The IP address must be on the same network as the TFTP server.
 Make sure that you do not enter the IP address of another device on this network.

9. Type T get the new firmware image from the TFTP server.
 The FortiGate unit loads the firmware.
10. Save the firmware as the default (D) or backup (B) firmware image, or run the image without saving it (R).
 The FortiGate unit installs the new firmware image and restarts. The installation might take a few minutes to complete.

Restoring from a USB drive

The FortiGate firmware can be manually restored from a USB drive, or installed automatically from a USB drive after a reboot.

To restore the firmware from a USB drive:

1. Copy the firmware file to the root directory on the USB drive.
2. Connect the USB drive to the USB port of the FortiGate device.
3. Connect to the FortiGate CLI using the RJ-45 to USB (or DB-9) or null modem cable.
4. Enter the following command:

```
execute restore image usb <filename>
```

The FortiGate unit responds with the following message:

```
This operation will replace the current firmware version! Do you want to continue?
(y/n)
```

5. Type y. The FortiGate unit restores the firmware and restarts. This process takes a few minutes.
 6. Update the antivirus and attack definitions:
- ```
execute update-now
```

**To install firmware automatically from a USB drive:**

1. Go to *System > Settings*.
2. In the *Start Up Settings* section, enable *Detect firmware* and enter the name of the firmware file.
3. Copy the firmware file to the root directory on the USB drive.
4. Connect the USB drive to the USB port of the FortiGate device.
5. Reboot the FortiGate device.

## Controlled upgrade

Using a controlled upgrade, you can upload a new version of the FortiOS firmware to a separate partition in the FortiGate memory for later upgrade. The FortiGate unit can be configured so that when it is rebooted, it will automatically load the new firmware. Using this option, you can stage multiple FortiGate units to upgrade simultaneously using FortiManager or a script.

**To load the firmware for later installation:**

```
execute restore secondary-image {ftp | tftp | usb} <filename_str>
```

**To set the FortiGate unit so that when it reboots, the new firmware is loaded:**

```
execute set-next-reboot {primary | secondary}
```

where {primary | secondary} is the partition with the preloaded firmware.

## Settings

The default administrator password should be configured immediately after the FortiGate is installed, see [Default administrator password on page 633](#).

After that, there are several system settings that should also be configured in *System > Settings*:

- [Changing the host name on page 633](#)
- [Setting the system time on page 634](#)
- [Configuring ports on page 637](#)
- [Setting the idle timeout time on page 638](#)
- [Setting the password policy on page 638](#)
- [Changing the view settings on page 638](#)
- [Setting the administrator password retries and lockout time on page 639](#)
- [TLS configuration on page 640](#)
- [Controlling return path with auxiliary session on page 641](#)
- [Email alerts on page 644](#)
- [Trusted platform module support on page 648](#)

## Default administrator password

By default, your FortiGate has an administrator account set up with the username `admin` and no password. In order to prevent unauthorized access to the FortiGate, it is highly recommended that you add a password to this account.



In FortiOS 6.2.1 and later, adding a password to the `admin` administrator is mandatory. You will be prompted to configure it the first time you log in to the FortiGate using that account, after a factory reset, and after a new image installation.

### To change the default password in the GUI:

1. Go to *System > Administrators*.
2. Edit the `admin` account.
3. Click *Change Password*.
4. If applicable, enter the current password in the *Old Password* field.
5. Enter a password in the *New Password* field, then enter it again in the *Confirm Password* field.
6. Click *OK*.

### To change the default password in the CLI:

```
config system admin
 edit admin
 set password <password>
 next
end
```



It is also recommended that you change the user name of this account; however, since you cannot change the user name of an account that is currently in use, a second administrator account must be created in order to do this.

## Changing the host name

The FortiGate host name is shown in the *Hostname* field in the *System Information* widget on a dashboard, as the command prompt in the CLI, as the SNMP system name, as the device name on FortiGate Cloud, and other places. If the FortiGate is in an HA cluster, use a unique host name to distinguish it from the other devices in the cluster.

An administrator requires *System > Configuration* read/write access to edit the host name. See [Administrator profiles on page 619](#) for details.

### To change the host name in the GUI:

1. Go to *System > Settings*.
2. In the *Host name* field, enter a new name.
3. Click *Apply*.

## To change the host name in the CLI:

```
config system global
 set hostname <hostname>
end
```

## Setting the system time

You can either manually set the FortiOS system time, or configure the device to automatically keep its system time correct by synchronizing with a Network Time Protocol (NTP) server.

Daylight savings time is enabled by default, and can only be configured in the CLI.



For many features to work, including scheduling, logging, and SSL-dependent features, the FortiOS system time must be accurate.

## To configure the date and time in the GUI:

1. Go to *System > Settings*.
2. In the *System Time* section, configure the following settings to either manually set the time or use an NTP server:

|                                         |                                                                                                                                                                                              |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Time Zone</b>                        | Select a time zone from the list. This should be the time zone that the FortiGate is in.                                                                                                     |
| <b>Set Time</b>                         | Select to either <i>Synchronize with an NTP Server</i> , or use <i>Manual settings</i> .                                                                                                     |
| <b>Synchronize with an NTP Server</b>   | To use an NTP server other than FortiGuard, the CLI must be used. In the <i>Sync interval</i> field, enter how often, in minutes, that the device synchronizes its time with the NTP server. |
| <b>Manual settings</b>                  | Manually enter the <i>Date</i> , <i>Hour</i> (in 24-hour format), <i>Minute</i> , and <i>Second</i> in their fields.                                                                         |
| <b>Setup device as local NTP server</b> | Enable to configure the FortiGate as a local NTP server. In the <i>Listen on Interfaces</i> field, set the interface or interfaces that the FortiGate will listen for NTP requests on.       |

3. Click *Apply*.

## To configure the date and time in the CLI:

1. Configure the timezone and daylight savings time:

```
config system global
 set timezone <integer>
 set dst {enable | disable}
end
```

2. Either manually configure the date and time, or configure an NTP server:

Manual:



```
execute date <yyyy-mm-dd>
execute time <hh:mm:ss>
```

**NTP server:**

```
config system ntp
 set ntpsync enable
 set type {fortiguard | custom}
 set syncinterval <integer>
 set source-ip <ip_address>
 set source-ip6 <ip6_address>
 set server-mode {enable | disable}
 set interface <interface>
 set authentication {enable | disable}
 set key-type {MD5 | SHA1}
 set key <password>
 set key-id <integer>
 config ntpserver
 edit <server_id>
 set server <ip_address or hostname>
 set ntpv3 {enable | disable}
 set authentication {enable | disable}
 set key <password>
 set key-id <integer>
 next
 end
end
```

## SHA-1 authentication support (for NTPv4)

SHA-1 authentication support allows the NTP client to verify that servers are known and trusted and not intruders masquerading (accidentally or intentionally) as legitimate servers. In cryptography, SHA-1 is a cryptographic hash algorithmic function.



SHA-1 authentication support is only available for NTP clients, not NTP servers.

---

**To configure authentication on a FortiGate NTP client:**

```
config system ntp
 set ntpsync enable
 set type custom
 set syncinterval 1
 config ntpserver
 edit "883502"
 set server "10.1.100.11"
 set authentication enable
 set key
 ENCi9NmcqsV3xBJv0kgIL3lFxA8mnNs2XKfB7spOQoUw4cm8FOOP0nrCbqx6rJ+om95+hVUHpaVZmepdd4KznPlAHNiu
 liPgPOk
 set key-id 1
 next
```

```
end
end
```

| Command                           | Description                                                             |
|-----------------------------------|-------------------------------------------------------------------------|
| authentication <enable   disable> | Enable/disable MD5/SHA1 authentication (default = disable).             |
| key <passwd>                      | Key for MD5/SHA1 authentication. Enter a password value.                |
| key-id <integer>                  | Key ID for authentication. Enter an integer value from 0 to 4294967295. |

### To confirm that NTP authentication is set up correctly:

```
diagnose sys ntp status
synchronized: yes, ntpsync: enabled, server-mode: disabled
ipv4 server(10.1.100.11) 10.1.100.11 -- reachable(0xff) S:4 T:6 selected
server-version=4, stratum=3
```

If NTP authentication is set up correctly, the server version is equal to 4.

## PTPv2

Precision time protocol (PTP) is used to synchronize network clocks. It is best suited to situations where time accuracy is of the utmost importance, as it supports accuracy in the sub-microsecond range. Conversely, NTP accuracy is in the range of milliseconds or tens of milliseconds.

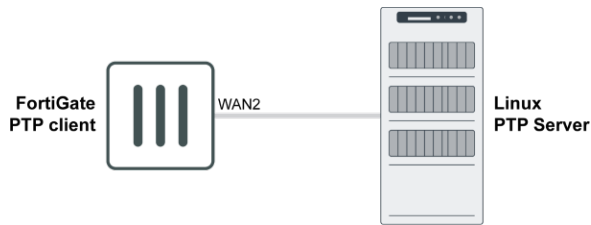
The following CLI commands are available:

```
config system ptp
 set status {enable | disable}
 set mode {multicast | hybrid}
 set delay-mechanism {E2E | P2P}
 set request-interval <integer>
 set interface <interface>
end
```

| Command                     | Description                                                                                                                 |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| status {enable   disable}   | Enable or disable the FortiGate system time by synchronizing with a PTP server (default = disable).                         |
| mode {multicast   hybrid}   | Use multicast or hybrid transmission (default = multicast).                                                                 |
| delay-mechanism {E2E   P2P} | Use end-to-end (E2E) or peer-to-peer (P2P) delay detection (default = E2E).                                                 |
| request-interval <integer>  | The logarithmic mean interval between the delay request messages sent by the client to the server in seconds (default = 1). |
| interface <interface>       | The interface that the PTP client will reply through.                                                                       |

### Sample configuration

This example uses the following topology:



**To configure a FortiGate to act as a PTP client that synchronizes itself with a Linux PTP server:**

1. Enable debug messages:  
`diagnose debug application ptpd -1`  
This command will provide details to debug the PTP communication with the server.
2. Check the system date:  
`execute date`  
current date is: 2019-01-01
3. Configure PTP in global mode:  
`config system ptp`  
    `set status enable`  
    `set interface wan2`  
`end`
4. Check the system date again after synchronization with the PTP server:  
`execute date`  
current date is: 2019-01-14

## Configuring ports

To improve security, the default ports for administrative connections to the FortiGate can be changed. Port numbers must be unique. If a conflict exists with a particular port, a warning message is shown.

When connecting to the FortiGate after a port has been changed, the port number be included, for example:  
`https://192.168.1.99:100`.

### To configure the ports in the GUI:

1. Go to *System > Settings*.
2. In the *Administration Settings* section, set the HTTP, HTTPS, SSH, and Telnet ports.
3. Enable *Redirect to HTTPS* to prevent HTTP from being used by administrators.
4. Click *Apply*.

### To configure the ports in the CLI:

```
config system global
 set admin-port <port>
 set admin-sport <port>
 set admin-https-redirect {enable | disable}
 set admin-ssh-port <port>
 set admin-telnet-port <port>
end
```

## Custom default service port range

The default service port range can be customized using the following CLI command:

```
config system global
 set default-service-source-port <port range>
end
```

Where <port range> is the new default service port range, that can have a minimum value of 0 and a maximum value up to 65535. The default value is 1 to 65535.



This change effects the TCP/UDP protocol.

---

## Setting the idle timeout time

The idle timeout period is the amount of time that an administrator will stay logged in to the GUI without any activity. This is to prevent someone from accessing the FortiGate if the management PC is left unattended. By default, it is set to five minutes.



A setting of higher than 15 minutes will have a negative effect on a security rating score. See [Security rating on page 133](#) for more information.

---

### To change the idle timeout in the GUI:

1. Go to *System > Settings*.
2. In the *Administration Settings* section, set the *Idle timeout* to up to 480 minutes.
3. Click *Apply*.

### To change the idle timeout in the CLI:

```
config system global
 set admintimeout <integer>
end
```

## Setting the password policy

A password policy can be created for administrators and IPsec pre-shared keys. See [Password policy on page 624](#) for information.

## Changing the view settings

The view settings change the look and language of the FortiOS GUI.

## To change the view settings in the GUI:

1. Go to *System > Settings*.
2. In the *View Settings* section, configure the following settings:

|                          |                                                                                                                                                                                    |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Language</b>          | Set the GUI language: <i>English, French, Spanish, Portuguese, Japanese, Traditional Chinese, Simplified Chinese, Korean.</i>                                                      |
| <b>Lines per page</b>    | Set the number of lines per page, from 20 to 100.                                                                                                                                  |
| <b>Theme</b>             | Set the theme color: <i>Green, Red, Blue, Melongene, or Mariner.</i>                                                                                                               |
| <b>Date/Time Display</b> | Set the date and time to display using the FortiGate's or the browser's timezone.                                                                                                  |
| <b>NGFW Mode</b>         | Set the NGFW mode to either <i>Profile-based</i> (default) or <i>Policy-based</i> .<br>If <i>Policy-based</i> is selected, the <i>SSL/SSH Inspection</i> profile must be selected. |

3. Click *Apply*.

## To change the view settings in the CLI:

```
config system global
 set language {english | french | spanish | portuguese | japanese | trach | simch |
korean}
 set gui-lines-per-page <integer>
 set gui-theme {green | red | blue | melongene | mariner}
 set gui-date-time-source {system | browser}
end
config system settings
 set ngfw-mode {profile-based | policy-based}
 set ssl-ssh-profile {certificate-inspection | custom-deep-inspection | deep-inspection |
no-inspection}
end
```

## Setting the administrator password retries and lockout time

By default, the number password retry attempts is set to three, allowing the administrator a maximum of three attempts at logging in to their account before they are locked out for a set amount of time (by default, 60 seconds).

The number of attempts and the default wait time before the administrator can try to enter a password again can be configured using the CLI.

A maximum of ten retry attempts can be configured, and the lockout period can be 1 to 2147483647 seconds (over 68 years). The higher the retry attempts, the higher the risk that someone might be able to guess the password.

## To configure the lockout options:

```
config system global
 set admin-lockout-threshold <failed_attempts>
 set admin-lockout-duration <seconds>
end
```

## Example:

To set the number of retry attempts to 1, and the lockout time to 5 minutes, enter the following commands:

```
config system global
 set admin-lockout-threshold 1
 set admin-lockout-duration 300
end
```



If the time span between the first failed log in attempt and the lockout threshold failed attempt is less than lockout time, the lockout will be triggered.

## TLS configuration

The minimum TLS version that is used for local out connections from the FortiGate can be configured in the CLI:

```
config system global
 set ssl-min-protocol-version {SSLv3 | TLSv1 | TLSv1-1 | TLSv1-2 | TLSv1-3}
end
```

By default, the minimum version is TLSv1.2. The FortiGate will try to negotiate a connection using the configured version or higher. If the server that FortiGate is connecting to does not support the version, then the connection will not be made. Some FortiCloud and FortiGuard services do not support TLSv1.3.

Minimum SSL/TLS versions can also be configured individually for the following settings, not all of which support TLSv1.3:

| Setting             | CLI                              |
|---------------------|----------------------------------|
| Email server        | config system email-server       |
| Certificate         | config vpn certificate setting   |
| FortiSandbox        | config system fortisandbox       |
| FortiGuard          | config log fortiguard setting    |
| FortiAnalyzer       | config log fortianalyzer setting |
| Syslog              | config log syslogd setting       |
| User Authentication | config user setting              |
| LDAP server         | config user ldap                 |
| POP3 server         | config user pop3                 |
| Exchange server     | config user exchange             |

A minimum (`ssl-min-protocol-ver`) and a maximum (`ssl-max-protocol-ver`) version can be configured for SSL VPN. See [TLS 1.3 support on page 1479](#)

## Controlling return path with auxiliary session

When multiple incoming or outgoing interfaces are used in ECMP or for load balancing, changes to routing, incoming, or return traffic interfaces impacts how an existing sessions handles the traffic. In FortiOS 6.2.3 and later, auxiliary sessions can be used to handle these changes to traffic patterns.

- In FortiOS 6.0 and earlier, the auxiliary session feature is not supported.
- In FortiOS 6.2.0 to 6.2.2, the auxiliary session feature is permanently enabled.
- In FortiOS 6.2.3 and later, the auxiliary session feature is disabled by default, and can be enabled if required.

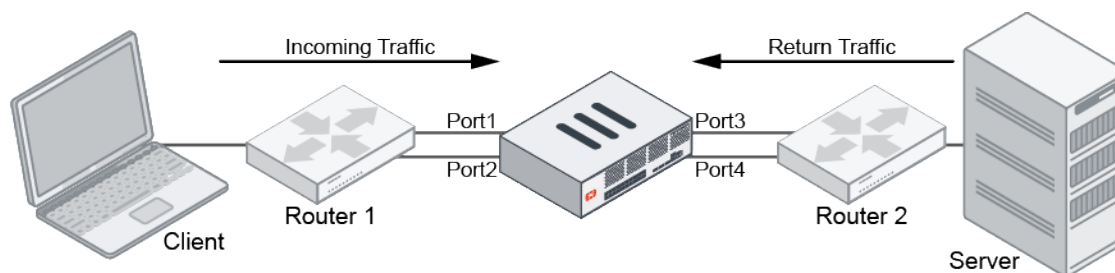
### To enable the auxiliary session feature:

```
config system settings
 set auxiliary-session {enable | disable*}
end
```



When enabling auxiliary sessions, consider the impact of routing in both traffic directions. In topologies such as SD-WAN hub and spoke or ADVPN deployments, the symmetry of the return traffic is important for maintaining the stability of the session. It is expected that the spoke selects the outbound interface and path, and the other nodes obey and reply symmetrically. It is recommended to disable auxiliary in these scenarios, and others where incoming and return traffic symmetry is expected.

## Scenarios



Incoming traffic is from the client to the server. Return traffic is from the server to the client.

### Scenario 1 - Return traffic returns on the original outgoing interface

In this scenario, a session is established between port1 and port3. When the return traffic hits port3:

#### Auxiliary sessions disabled:

The reply to the client egresses on the original incoming interface, port1. If policy routes or SD-WAN rules are configured, the next hop gateway is applied if the output device is the same as the original incoming interface.

#### Auxiliary sessions enabled:

The reply to the client egresses on the best route in the routing table:

- If the best route is port1, then it will egress on port1.
- If the best route is port2, then it will egress on port2.

If policy routes or SD-WAN rules are configured, they must be matched to determine the egress interface. If both are configured, policy routes have higher priority.

## Scenario 2 - Return traffic returns on an interfaces other than the original outgoing interfaces

In this scenario, a session is established between port1 and port3. When the return traffic hits port4:

### Auxiliary sessions disabled:

- The session is dirtied and then gets refreshed, and interfaces on the session are updated.
- If there is a high traffic volume or flapping between the interfaces, the CPU usage increases.

### Auxiliary sessions enabled:

An auxiliary session is created for the existing session, and traffic returns to the client as normal on the auxiliary session.

## Scenario 3 - Incoming traffic enters on an interfaces other than the original incoming interfaces

In this scenario, a session is established between port1 and port3. When the incoming traffic hits port2:

### Auxiliary sessions disabled:

The session is dirtied and then gets refreshed, and interfaces on the session are updated.

### Auxiliary sessions enabled:

An auxiliary session is created for the existing session, and traffic is forwarded to the server as normal on the auxiliary session.

## Scenario 4 - the routing table is changed

In this scenario, a session has been established between port1 and port3, when a new route on port4 is updated as the route to the server.

### Auxiliary sessions disabled:

As long as there is a route to the destination, the session will not be dirtied or refreshed. Even though there is a better route, traffic continues on the original path between port1 and port3.

### Auxiliary sessions enabled:

The session is dirtied and then gets refreshed, and interfaces on the session are updated.

## Effect on NPU offloading sessions

When the auxiliary session feature is disabled, there is always one session. If the incoming or return interface changes, the FortiGate marks the session as dirty and updates the session's interfaces. This cannot be done by the NPU, so the



session is not offloaded to the NPU, and is processed by the CPU instead. If Equal-Cost Multi-Path (ECMP) causes the interface to keep changing, then it will use significant CPU resources.

When the auxiliary session feature is enabled and the incoming or return interface changes, it creates an auxiliary session, and all traffic can continue to be processed by the NPU.

## Verification

When an auxiliary, or reflect, session is created, it will appear as a reflect session below the existing session:

```
diagnose sys session list
session info: proto=17 proto_state=00 duration=111 expire=175 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=131/4/1 reply=0/0/0 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=36->38/38->36 gwy=10.1.2.3/0.0.0.0
hook=pre dir=org act=noop 10.1.100.22:51926->172.16.204.44:5001(0.0.0.0:0)
hook=post dir=reply act=noop 172.16.204.44:5001->10.1.100.22:51926(0.0.0.0:0)
src_mac=90:6c:ac:19:19:58
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=2
serial=00002b11 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpd_b_link_id=00000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x000400
npu info: flag=0x91/0x00, offload=8/0, ips_offload=0/0, epid=129/0, ipid=142/0,
vlan=0x0016/0x0000
vlifid=142/0, vtag_in=0x0016/0x0000 in_npu=1/0, out_npu=1/0, fwd_en=0/0, qid=4/0
no_ofld_reason:
reflect info 0:
dev=37->38/38->37
npu_state=0x000400
npu info: flag=0x91/0x00, offload=8/0, ips_offload=0/0, epid=129/0, ipid=142/0,
vlan=0x0017/0x0000
vlifid=142/0, vtag_in=0x0017/0x0000 in_npu=1/0, out_npu=1/0, fwd_en=0/0, qid=4/0
total reflect session num: 1
total session 1
```

When a session is dirtied, a dirty flag is added to it:

```
diagnose sys session list
session info: proto=17 proto_state=00 duration=28 expire=152 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=dirty may_dirty npu
statistic(bytes/packets/allow_err): org=68/2/1 reply=0/0/0 tuples=2
tx speed(Bps/kbps): 2/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=0->0/0->0 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.1.100.22:51926->172.16.204.44:5001(0.0.0.0:0)
```

```
hook=post dir=reply act=noop 172.16.204.44:5001->10.1.100.22:51926(0.0.0.0:0)
src_mac=90:6c:ac:19:19:58 dst_mac=02:6c:ac:5c:c6:f9
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=2
serial=00002b2c tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpd_b_link_id=00000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x000400
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0,
vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
total session 1
```

When an auxiliary session is created, NPU offloading will continue in the reflect session:

```
diagnose sys session list
session info: proto=17 proto_state=01 duration=169 expire=129 timeout=0 flags=00000000
socktype=0 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu
statistic(bytes/packets/allow_err): org=131/4/1 reply=66/2/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=36->38/38->36 gwy=10.1.2.3/172.17.2.1
hook=pre dir=org act=noop 10.1.100.22:51926->172.16.204.44:5001(0.0.0.0:0)
hook=post dir=reply act=noop 172.16.204.44:5001->10.1.100.22:51926(0.0.0.0:0)
src_mac=90:6c:ac:19:19:58
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=2
serial=00002b11 tos=ff/ff app_list=0 app=0 url_cat=0
sdwan_mbr_seq=0 sdwan_service_id=0
rpd_b_link_id=00000000 rpd_b_svc_id=0 ngfwid=n/a
npu_state=0x000c00
npu info: flag=0x91/0x81, offload=8/8, ips_offload=0/0, epid=129/142, ipid=142/128,
vlan=0x0016/0x0016
vlifid=142/128, vtag_in=0x0016/0x0016 in_npu=1/1, out_npu=1/1, fwd_en=0/0, qid=4/4
reflect info 0:
dev=37->38/38->37
npu_state=0x000400
npu info: flag=0x91/0x00, offload=8/0, ips_offload=0/0, epid=129/0, ipid=142/0,
vlan=0x0017/0x0000
vlifid=142/0, vtag_in=0x0017/0x0000 in_npu=1/0, out_npu=1/0, fwd_en=0/0, qid=4/0
total reflect session num: 1
total session 1
```

## Email alerts

Alert emails are used to notify administrators about events on the FortiGate device, allowing a quick response to any issues.

There are two methods that can be used to configure email alerts:

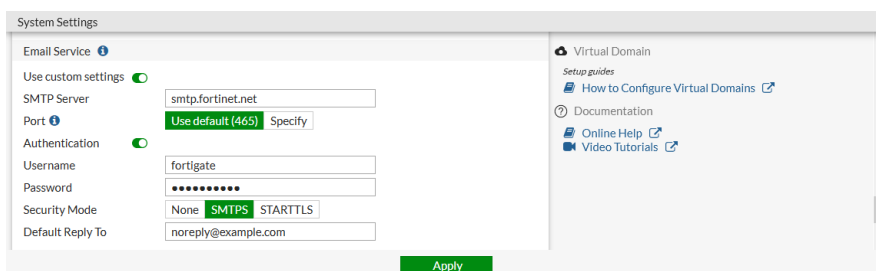
- [Automation stitches on page 645](#)
- [Alert emails on page 647](#)

The FortiGate has a default SMTP server, `notification.fortinet.net`, that provides secure mail service with SMTPS. It is used for all emails that are sent by the FortiGate, including alert emails, automation stitch emails, and FortiToken Mobile activations. You can also configure a custom email service.

### To configure a custom email service in the GUI:

1. Go to *System > Settings*.
2. In the *Email Service* section, enable *Use custom settings*.
3. Configure the following settings:

|                         |                                                                                                                                                                          |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SMTP Server</b>      | Enter the address or name of the SMTP server, such as <i>smtp.example.com</i> .                                                                                          |
| <b>Port</b>             | If required, select <i>Specify</i> and enter a specific port number. The default is port 465.                                                                            |
| <b>Authentication</b>   | If required by the email server, enable authentication.<br>If enabled, enter the <i>Username</i> and <i>Password</i> .                                                   |
| <b>Security Mode</b>    | Set the security mode: <i>None</i> , <i>SMTPS</i> , or <i>STARTTLS</i> .                                                                                                 |
| <b>Default Reply To</b> | Optionally, enter the reply to email address, such as <i>noreply@example.com</i> .<br>This address will override the from address that is configured for an alert email. |



4. Click *Apply*.

### To configure a custom email service in the CLI:

```
config system email-server
 set reply-to "noreply@example.com"
 set server "smtp.fortinet.net"
 set port 465
 set authenticate enable
 set username "fortigate"
 set password *****
 set security smtps
end
```

## Automation stitches

Automation stitches can be configured to send emails based on a variety of triggers, giving you control over the events that cause an alert, and who gets alerted. For more information, see [Automation stitches on page 233](#).

In this example, the default mail service sends an email to two recipients when there is a configuration change or an Admin login failed event occurs.

### To configure the automation stitch in the GUI:

1. On the root FortiGate, go to *Security Fabric > Automation* and click *Create New*.
2. Enter a name for the stitch, such as *Admin Fail*.
3. In the *Trigger* section, select *FortiOS Event Log*.
4. Click in the *Event* field, and in the slide out pane, search for and select *Admin login failed*.
5. In the *Action* section, select *Email*.
6. Configure the *Email* settings:
  - a. In the *To* field, click the plus icon, then enter the two email recipients' addresses, such as *admin@example.com* and *manager@example.com*.
  - b. Enter the *Email subject*, such as *Admin log in failed*.
  - c. Edit the *Email body* as required. By default, the email body will include all the fields from the log event that triggered the stitch.

New Automation Stitch

Name: Admin Fail

Status: + Enabled - Disabled

Trigger

FortiOS Event Log

Event: Admin login failed

Action

CLI Script, Email, FortiExplorer Notification, AWS Lambda, Azure Function, Google Cloud Function, AllCloud Function, Slack Notification, Webhook

Minimum Interval (seconds): 0

Email

To: admin@example.com, manager@example.com

Email subject: Admin log in failed

Email body: %%log%%

OK Cancel

7. Click *OK*.
8. Create a second stitch, selecting *Configuration Change* as the trigger.

### To configure the automation stitch in the CLI:

1. Create automation actions to send the email messages:

```
config system automation-action
 edit "Config Change_email"
 set action-type email
 set email-to "admin@example.com" "manager@example.com"
 set email-subject "Configuration Change Detected"
 next
 edit "Admin Fail_email"
```

```
 set action-type email
 set email-to "admin@example.com" "manager@example.com"
 set email-subject "Admin log in failed"
 next
end
```

## 2. Create the automation triggers:

```
config system automation-trigger
 edit "Config Change"
 set event-type config-change
 next
 edit "Admin Fail"
 set event-type event-log
 set logid 32002
 next
end
```

## 3. Create the automation stitches:

```
config system automation-stitch
 edit "Config Change"
 set trigger "Config Change"
 set action "Config Change_email"
 next
 edit "Admin Fail"
 set trigger "Admin Fail"
 set action "Admin Fail_email"
 next
end
```

## Alert emails

When configuring an alert email, you can define the threshold when an issue becomes critical and requires attention. When the threshold is reached, an email is sent to up to three recipients on the configured schedule to notify them of the issue.

In this example, the FortiGate is configured to send email messages to two addresses, admin@example.com and manager@example.com, every two minutes when multiple intrusions, administrator log in or out events, or configuration changes occur.

### To configure an alert email in the GUI:

1. Go to *Log & Report > Email Alert Settings* and enable *Enabled*.
2. Configure the following:

|                        |                                                                                                               |
|------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>From</b>            | Enter the name in the <i>From</i> field of the message: fortigate@example.com.                                |
| <b>To</b>              | Enter the two addresses that the message is sent to: admin@example.com and manager@example.com                |
| <b>Alert parameter</b> | Send the alert based on specific events ( <i>category</i> ), as opposed to the severity ( <i>threshold</i> ). |
| <b>Interval</b>        | Set the interval between messages to 2 minutes.                                                               |

**Security** Enable *Intrusion detected* (IPS-logs).

**Administrative** Enable *Administrator login/logout* (admin-login-logs) and *Configuration change* (configuration-changes-logs).

Email Alert Settings

Enabled ☒

From: fortigate@example.com

To: admin@example.com, manager@example.com

Alert parameter: Events, Severity

Interval: 2

**Security**

Intrusion detected ☒

Virus detected ☐

Web Filter blocked traffic ☐

Policy denied traffic ☐

**Administrative**

FortiGuard renewal due within ☐

Administrator login/logout ☒

Configuration change ☒

Firewall authentication failure ☐

HA status change ☐

Apply

3. Click *Apply*.

### To configure an alert email in the CLI:

```
config alertemail setting
 set username fortigate@example.com
 set mailto1 admin@example.com
 set mailto2 manager@example.com
 set filter-mode category
 set email-interval 2
 set IPS-logs enable
 set configuration-changes-logs enable
 set admin-login-logs enable
end
```

For more information on the available CLI commands, see [Configure alert email settings](#).

## Trusted platform module support

On supported FortiGate hardware devices, the Trusted Platform Module (TPM) can be used to protect your password and key against malicious software and phishing attacks. The dedicated module hardens the FortiGate by generating, storing, and authenticating cryptographic keys. To help prevent tampering, the chip is soldered on the motherboard to reduce the risk of data transaction interceptions from attackers.

By default, the TPM is disabled. To enable it, you must set the 32 hexadecimal digit master-encryption-password which encrypts sensitive data on the FortiGate using AES128-CBC. With the password, TPM generates a 2048-bit primary key to secure the master-encryption-password through RSA-2048 encryption. The master-encryption-password protects the data. The primary key protects the master-encryption-password.



The TPM module does not encrypt the disk drive of eligible FortiGate.

---

The primary key binds the encrypted configuration file to a specific FortiGate unit and never leaves the TPM. When backing up the configuration, the TPM uses the primary key to encrypt the master-encryption-password in the configuration file. When restoring a configuration that includes a TPM protected master-encryption-password:

- If TPM is disabled, then the configuration cannot be restored.
- If TPM is enabled but has a different master-encryption-password than the configuration file, then the configuration cannot be restored.
- If TPM is enabled and the master-encryption-password is the same in the configuration file, then the configuration can be restored.

For information on backing up and restoring the configuration, see [Configuration backups on page 62](#).

Passwords and keys that can be encrypted by the master-encryption-key include:

- Admin password
- Alert email user's password
- BGP and other routing related configurations
- External resource
- FortiGuard proxy password
- FortiToken/FortiToken Mobile's seed
- HA password
- IPsec pre-shared key
- Link Monitor, server side password
- Local certificate's private key
- Local, LDAP, RADIUS, FSSO, and other user category related passwords
- Modem/PPPoE
- NST password
- NTP Password
- SDN connector, server side password
- SNMP
- Wireless Security related password



In HA configurations, each cluster member must use the same master-encryption-key so that the HA cluster can form and its members can synchronize their configurations.

---

### To check if your FortiGate device has a TPM:

Verify all the following commands exist. Otherwise, the platform does not support it.

```
diagnose hardware test info
List of test cases:
 bios: sysid
 bios: checksum
```

```
 bios: license
 bios: detect

diagnose hardware deviceinfo tpm
TPM capability information of fixed properties:
=====
TPM_PT_FAMILY_INDICATOR: 2.0
TPM_PT_LEVEL: 0
TPM_PT_REVISION: 138
TPM_PT_DAY_OF_YEAR: 8
TPM_PT_YEAR: 2018
TPM_PT_MANUFACTURER: NTC
diagnose hardware test tpm
===== Fortinet Hardware Test Report =====
TPM
TPM Device Detection..... PASS
===== Fortinet Hardware Test PASSED =====
diagnose tpm
get-property Get TPM properties. [Take 0-1 arg(s)]
get-var-property Get TPM var properties.
read-clock Read TPM internal clock.
shutdown-prepare Prepare for TPM power cycle.
selftest Perform self tests.
generate-random-number Generate a 4-byte random number
SHA-1 HASH a sequence of num with SHA-1 algo
SHA-256 HASH a sequence of num with SHA-256 algo
```

**To enable TPM and input the master-encryption-password:**

```
config system global
 set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):

Please re-enter your private data encryption key (32 hexadecimal numbers) again:

Your private data encryption key is accepted.
```

## Virtual Domains

Virtual Domains (VDOMs) are used to divide a FortiGate into two or more virtual units that function independently. VDOMs can provide separate security policies and, in NAT mode, completely separate configurations for routing and VPN services for each connected network.

There are two VDOM modes:

- Split-task VDOM mode: One VDOM is used only for management, and the other is used to manage traffic. See [Split-task VDOM mode on page 651](#).
- Multi VDOM mode: Multiple VDOMs can be created and managed as independent units. See [Multi VDOM mode on page 655](#).

By default, most FortiGate units support 10 VDOMs, and many FortiGate models support purchasing a license key to increase the maximum number.



Global settings are configured outside of a VDOM. They effect the entire FortiGate, and include settings such as interfaces, firmware, DNS, some logging and sandboxing options, and others. Global settings should only be changed by top level administrators.

## Switching VDOM modes

| Current VDOM mode | New VDOM mode   | Rule                                                                                                                                                                              |
|-------------------|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No VDOM           | Split-task VDOM | Allowed                                                                                                                                                                           |
| Split-task VDOM   | No VDOM         | Allowed                                                                                                                                                                           |
| No VDOM           | Multi VDOM      | Allowed only if the FortiGate is not a member of a Security Fabric. See <a href="#">Configuring the root FortiGate and downstream FortiGates on page 70</a> for more information. |
| Multi VDOM        | No VDOM         | Allowed                                                                                                                                                                           |
| Split-task VDOM   | Multi VDOM      | Allowed only if the FortiGate is not a member of a Security Fabric. See <a href="#">Configuring the root FortiGate and downstream FortiGates on page 70</a> for more information. |
| Multi VDOM        | Split-task VDOM | Not Allowed. User must first switch to <i>No VDOM</i>                                                                                                                             |

## Split-task VDOM mode

In split-task VDOM mode, the FortiGate has two VDOMs: the management VDOM (*root*) and the traffic VDOM (*FG-traffic*).



The management VDOM is used to manage the FortiGate, and cannot be used to process traffic.

The following GUI sections are available when in the management VDOM:

- The Status dashboard
- Security Fabric topology and settings (read-only, except for *HTTP Service* settings)
- Interface and static route configuration
- FortiClient configuration
- Replacement messages
- Certificates
- System events
- Log and email alert settings
- Threat weight definitions

The traffic VDOM provides separate security policies, and is used to process all network traffic.

The following GUI sections are available when in the traffic VDOM:

- The Status, Top Usage LAN/DMZ, and Security dashboards
- Security Fabric topology, settings (read-only, except for *HTTP Service* settings), and Fabric Connectors (SSO/*Identity* connectors only)
- FortiView
- Interface configuration
- Packet capture
- SD-WAN, SD-WAN Rules, and Performance SLA
- Static and policy routes
- RIP, OSPF, BGP, and Multicast
- Replacement messages
- Feature visibility
- Tags
- Certificates
- Policies and objects
- Security profiles
- VPNs
- User and device authentication
- Wifi and switch controller
- Logging
- Monitoring

Split-task VDOM mode is not available on all FortiGate models. The Fortinet Security Fabric supports split-task VDOM mode.

### Enable split-task VDOM mode

Split-task VDOM mode can be enabled in the GUI or CLI. Enabling it does not require a reboot, but does log you out of the FortiGate.



When split-task VDOM mode is enabled, all current management configuration is assigned to the *root* VDOM, and all non-management settings, such as firewall policies and security profiles, are deleted.

---

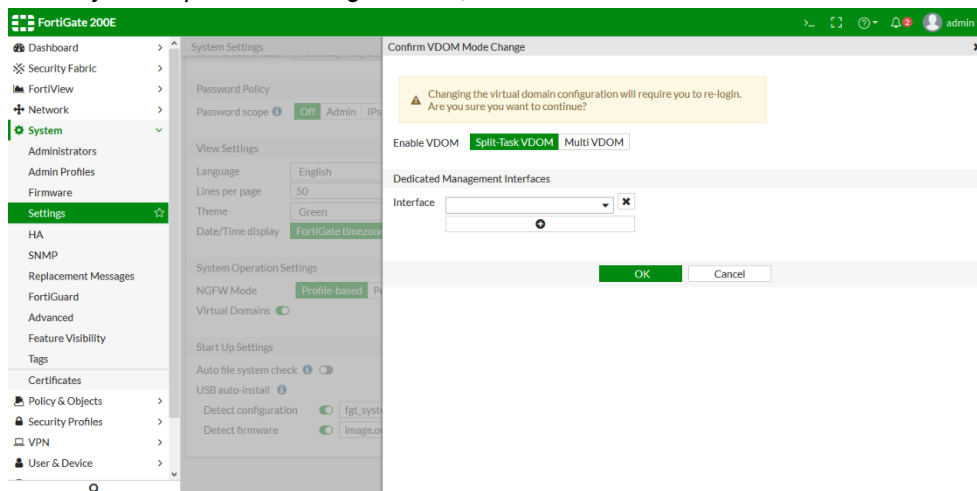


On FortiGate 60 series models and lower, VDOMs can only be enabled using the CLI.

---

### To enable split-task VDOM mode in the GUI:

1. On the FortiGate, go to *System > Settings*.
2. In the *System Operation Settings* section, enable *Virtual Domains*.



3. Select *Split-Task VDOM* for the VDOM mode.
4. Select a *Dedicated Management Interface* from the *Interface* list. This interface is used to access the management VDOM, and cannot be used in firewall policies.
5. Click **OK**.

### To enable split-task VDOM mode with the CLI:

```
config system global
 set vdom-mode split-vdom
end
```

## Assign interfaces to a VDOM

An interface can only be assigned to one of the VDOMs. When split-task VDOM mode is enabled, all interfaces are assigned to the *root* VDOM. To use an interface in a policy, it must first be assigned to the traffic VDOM.

An interface cannot be moved if it is referenced in an existing configuration.

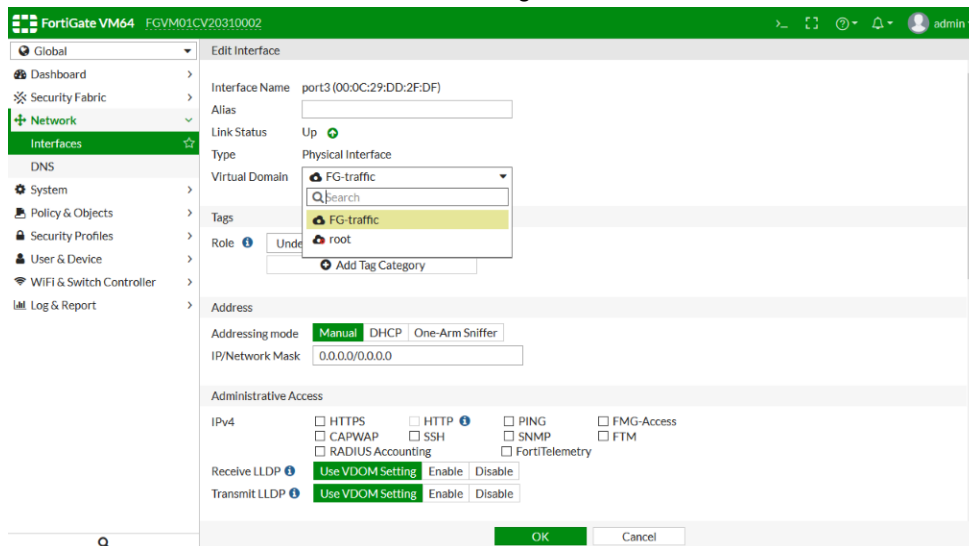


In the GUI, the interface list *Ref.* column shows if the interface is referenced in an existing configuration, and allows you to quickly access and edit those references.

### To assign an interface to a VDOM in the GUI:

1. On the FortiGate, go to *Global > Network > Interfaces*.
2. Edit the interface that will be assigned to a VDOM.

3. Select the VDOM that the interface will be assigned to from the *Virtual Domain* list.



4. Click **OK**.

#### To assign an interface to a VDOM using the CLI:

```
config global
 config system interface
 edit <interface>
 set vdom <VDOM_name>
 next
 end
end
```

## Create per-VDOM administrators

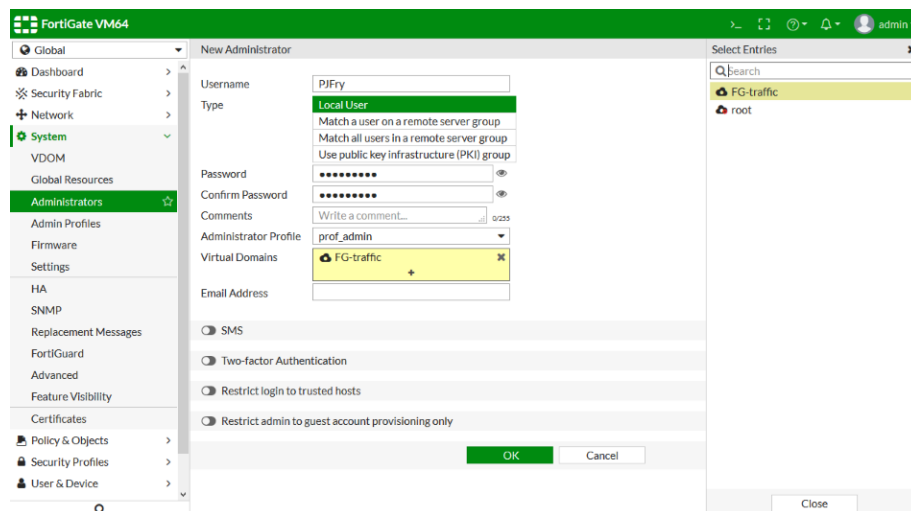
Per-VDOM administrators can be created that can access only the management or traffic VDOM. These administrators must use either the *prof\_admin* administrator profile, or a custom profile.

A per-VDOM administrator can only access the FortiGate through a network interface that is assigned to the VDOM that they are assigned to. The interface must also be configured to allow management access. They can also connect to the FortiGate using the console port.

To assign an administrator to multiple VDOMs, they must be created at the global level. When creating an administrator at the VDOM level, the *super\_admin* administrator profile cannot be used.

#### To create a per-VDOM administrator in the GUI:

1. On the FortiGate, connect to the management VDOM.
2. Go to *Global > System > Administrators* and click *Create New > Administrator*.
3. Fill in the required information, setting the *Type* as *Local User*.
4. In the *Virtual Domains* field, add the VDOM that the administrator will be assigned to, and if necessary, remove the other VDOM from the list.



5. Click OK.

### To create a per-VDOM administrator using the CLI:

```
config global
 config system admin
 edit <name>
 set vdom <VDOM_name>
 set password <password>
 set accprofile <admin_profile>
 ...
 next
 end
end
```

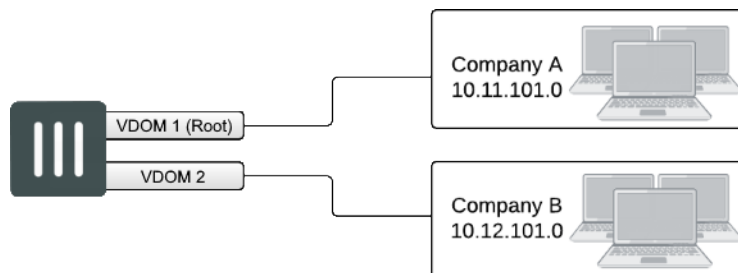
## Multi VDOM mode

In multi VDOM mode, the FortiGate can have multiple VDOMs that function as independent units. One VDOM is used to manage global settings. The root VDOM cannot be deleted, and remains in the configuration even if it is not processing any traffic.

Multi VDOM mode isn't available on all FortiGate models. The Fortinet Security Fabric does not support multi VDOM mode.

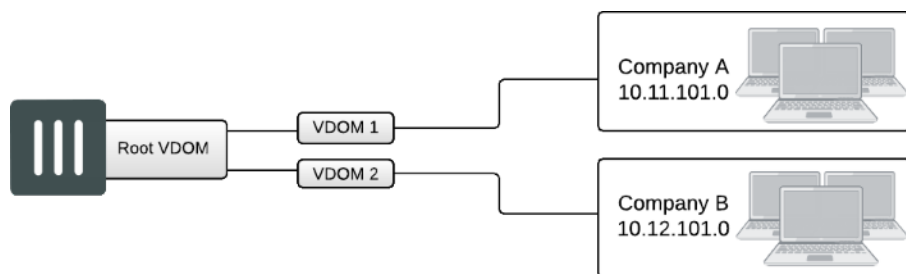
There are three main configuration types in multi VDOM mode:

### Independent VDOMs:



Multiple, completely separate VDOMs are created. Any VDOM can be the management VDOM, as long as it has Internet access. There are no inter-VDOM links, and each VDOM is independently managed.

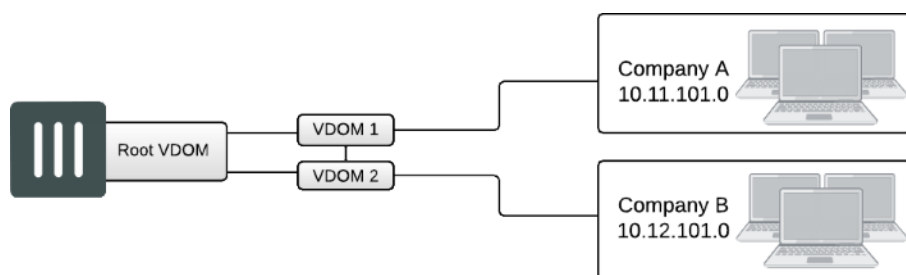
### Management VDOM:



A management VDOM is located between the other VDOMs and the Internet, and the other VDOMs connect to the management VDOM with inter-VDOM links. The management VDOM has complete control over Internet access, including the types of traffic that are allowed in both directions. This can improve security, as there is only one point of ingress and egress.

There is no communication between the other VDOMs.

### Meshed VDOMs:



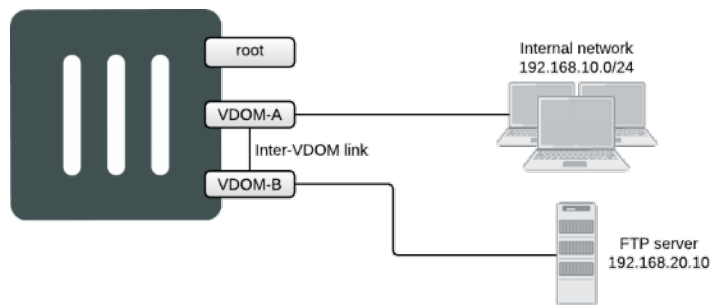
VDOMs can communicate with inter-VDOM links. In full-mesh configurations, all the VDOMs are interconnected. In partial-mesh configurations, only some of the VDOMs are interconnected.

In this configuration, proper security must be achieved by using firewall policies and ensuring secure account access for administrators and users.

## Multi VDOM configuration examples

The following examples show how to configure per-VDOM settings, such as operation mode, routing, and security policies, in a network that includes the following VDOMs:

- VDOM-A: allows the internal network to access the Internet.
- VDOM-B: allows external connections to an FTP server.
- root: the management VDOM.



You can use VDOMs in either NAT or transparent mode on the same FortiGate. By default, VDOMs operate in NAT mode.

For both examples, multi VDOM mode must be enabled, and VDOM-A and VDOM-B must be created.

### Enable multi VDOM mode

Multi VDOM mode can be enabled in the GUI or CLI. Enabling it does not require a reboot, but does log you out of the device. The current configuration is assigned to the *root* VDOM.



On FortiGate 60 series models and lower, VDOMs can only be enabled using the CLI.

#### To enable multi VDOM mode in the GUI:

1. On the FortiGate, go to *System > Settings*.
2. In the *System Operation Settings* section, enable *Virtual Domains*.
3. Select *Multi VDOM* for the VDOM mode.
4. Click *OK*.

#### To enable multi VDOM mode with the CLI:

```
config system global
 set vdom-mode multi-vdom
end
```

### Create the VDOMs

#### To create the VDOMs in the GUI:

1. In the *Global VDOM*, go to *System > VDOM*, and click *Create New*. The *New Virtual Domain* page opens.

2. In the *Virtual Domain* field, enter *VDOM-A*.

3. If required, set the *NGFW Mode*. If the *NGFW Mode* is *Policy-based*, select an *SSL/SSH Inspection* from the list.
4. Optionally, enter a comment.
5. Click *OK* to create the VDOM.
6. Repeat the above steps for *VDOM-B*.

#### To create the VDOMs with the CLI:

```
config vdom
 edit <VDOM-A>
 next
 edit <VDOM-B>
 next
end
end
```

### NAT mode

In this example, both VDOM-A and VDOM-B use NAT mode. A VDOM link is created that allows users on the internal network to access the FTP server.

This configuration requires the following steps:

1. [Configure VDOM-A on page 658](#)
2. [Configure VDOM-B on page 660](#)
3. [Configure the VDOM link on page 663](#)

## Configure VDOM-A

VDOM-A allows connections from devices on the internal network to the Internet. WAN 1 and port 1 are assigned to this VDOM.

The per-VDOM configuration for VDOM-A includes the following:

- A firewall address for the internal network
- A static route to the ISP gateway
- A security policy allowing the internal network to access the Internet

All procedures in this section require you to connect to VDOM-A, either using a global or per-VDOM administrator account.

#### To add the firewall addresses in the GUI:

1. Go to *Policy & Objects > Addresses* and create a new address.
2. Enter the following information:

|                             |                            |
|-----------------------------|----------------------------|
| <b>Name</b>                 | internal-network           |
| <b>Type</b>                 | Subnet                     |
| <b>Subnet / IP Range</b>    | 192.168.10.0/255.255.255.0 |
| <b>Interface</b>            | port1                      |
| <b>Show in Address List</b> | enabled                    |



**To add the firewall addresses with the CLI:**

```
config vdom
 edit VDOM-A
 config firewall address
 edit internal-network
 set associated-interface port1
 set subnet 192.168.10.0 255.255.255.0
 next
 end
 next
end
```

**To add a default route in the GUI:**

1. Go to *Network > Static Routes* and create a new route.
2. Enter the following information:

|                    |                 |
|--------------------|-----------------|
| <b>Destination</b> | Subnet          |
| <b>IP address</b>  | 0.0.0.0/0.0.0.0 |
| <b>Gateway</b>     | 172.20.201.7    |
| <b>Interface</b>   | wan1            |
| <b>Distance</b>    | 10              |

**To add a default route with the CLI:**

```
config vdom
 edit VDOM-A
 config router static
 edit 0
 set gateway 172.20.201.7
 set device wan1
 next
 end
 next
end
```

**To add the security policy in the GUI:**

1. Connect to VDOM-A.
2. Go to *Policy & Objects > IPv4 Policy* and create a new policy.
3. Enter the following information:

|                           |                  |
|---------------------------|------------------|
| <b>Name</b>               | VDOM-A-Internet  |
| <b>Incoming Interface</b> | port1            |
| <b>Outgoing Interface</b> | wan1             |
| <b>Source Address</b>     | internal-network |

|                            |         |
|----------------------------|---------|
| <b>Destination Address</b> | all     |
| <b>Schedule</b>            | always  |
| <b>Service</b>             | ALL     |
| <b>Action</b>              | ACCEPT  |
| <b>NAT</b>                 | enabled |

### To add the security policy with the CLI:

```
config vdom
 edit VDOM-A
 config firewall policy
 edit 0
 set name VDOM-A-Internet
 set srcintf port1
 set dstintf wan1
 set srcaddr internal-network
 set dstaddr all
 set action accept
 set schedule always
 set service ALL
 set nat enable
 next
 end
 next
end
```

## Configure VDOM-B

VDOM-B allows external connections to reach an internal FTP server. WAN 2 and port 2 are assigned to this VDOM.

The per-VDOM configuration for VDOM-B includes the following:

- A firewall address for the FTP server
- A virtual IP address for the FTP server
- A static route to the ISP gateway
- A security policy allowing external traffic to reach the FTP server

All procedures in this section require you to connect to VDOM-B, either using a global or per-VDOM administrator account.

### To add the firewall addresses in the GUI:

1. Go to *Policy & Objects > Addresses* and create a new address.
2. Enter the following information:

|                     |            |
|---------------------|------------|
| <b>Address Name</b> | FTP-server |
| <b>Type</b>         | Subnet     |

|                             |                  |
|-----------------------------|------------------|
| <b>Subnet / IP Range</b>    | 192.168.20.10/32 |
| <b>Interface</b>            | port2            |
| <b>Show in Address List</b> | enabled          |

#### To add the firewall addresses with the CLI:

```
config vdom
 edit VDOM-B
 config firewall address
 edit FTP-server
 set associated-interface port2
 set subnet 192.168.20.10 255.255.255.255
 next
 end
 next
end
```

#### To add the virtual IP address in the GUI:

1. Go to *Policy & Objects > Virtual IPs* and create a new virtual IP address.
2. Enter the following information:

|                                  |                |
|----------------------------------|----------------|
| <b>Name</b>                      | FTP-server-VIP |
| <b>Interface</b>                 | wan2           |
| <b>External IP Address/Range</b> | 172.25.177.42  |
| <b>Internal IP Address/Range</b> | 192.168.20.10  |

#### To add the virtual IP address with the CLI:

```
config firewall vip
 edit FTP-server-VIP
 set extip 172.25.177.42
 set extintf wan2
 set mappedip 192.168.20.10
 next
end
```

#### To add a default route in the GUI:

1. Go to *Network > Static Routes* and create a new route.
2. Enter the following information:

|                    |                 |
|--------------------|-----------------|
| <b>Destination</b> | Subnet          |
| <b>IP address</b>  | 0.0.0.0/0.0.0.0 |
| <b>Gateway</b>     | 172.20.10.10    |
| <b>Interface</b>   | wan2            |
| <b>Distance</b>    | 10              |

**To add a default route with the CLI:**

```
config vdom
 edit VDOM-B
 config router static
 edit 0
 set device wan2
 set gateway 172.20.10.10
 next
 end
 next
end
```

**To add the security policy in the GUI:**

1. Go to *Policy & Objects > IPv4 Policy* and create a new policy.
2. Enter the following information:

|                            |                |
|----------------------------|----------------|
| <b>Name</b>                | Access-server  |
| <b>Incoming Interface</b>  | wan2           |
| <b>Outgoing Interface</b>  | port2          |
| <b>Source Address</b>      | all            |
| <b>Destination Address</b> | FTP-server-VIP |
| <b>Schedule</b>            | always         |
| <b>Service</b>             | FTP            |
| <b>Action</b>              | ACCEPT         |
| <b>NAT</b>                 | enabled        |

**To add the security policy with the CLI:**

```
config vdom
 edit VDOM-B
 config firewall policy
 edit 0
 set name Access-server
 set srcintf wan2
 set dstintf port2
 set srcaddr all
 set dstaddr FTP-server-VIP
 set action accept
 set schedule always
 set service FTP
 set nat enable
 next
 end
 next
end
```

## Configure the VDOM link

The VDOM link allows connections from VDOM-A to VDOM-B. This allows users on the internal network to access the FTP server through the FortiGate.

The configuration for the VDOM link includes the following:

- The VDOM link interface
- Firewall addresses for the FTP server on VDOM-A and for the internal network on VDOM-B
- Static routes for the FTP server on VDOM-A and for the internal network on VDOM-B
- Policies allowing traffic using the VDOM link

All procedures in this section require you to connect to the global VDOM using a global administrator account.

### To add the VDOM link in the GUI:

1. Connect to root.
2. Go to **Global > Network > Interfaces** and select **Create New > VDOM link**.
3. Enter the following information:

|                       |                 |
|-----------------------|-----------------|
| <b>Name</b>           | VDOM-link       |
| <b>Interface 0</b>    |                 |
| <b>Virtual Domain</b> | VDOM-A          |
| <b>IP/Netmask</b>     | 0.0.0.0/0.0.0.0 |
| <b>Interface 1</b>    |                 |
| <b>Virtual Domain</b> | VDOM-B          |
| <b>IP/Netmask</b>     | 0.0.0.0/0.0.0.0 |

### To add the VDOM link with the CLI:

```
config global
 config system vdom-link
 edit vlink
 end
 config system interface
 edit VDOM-link0
 set vdom VDOM-A
 set ip 0.0.0.0 0.0.0.0
 next
 edit VDOM-link1
 set vdom VDOM-B
 set ip 0.0.0.0 0.0.0.0
 next
 end
end
```

### To add the firewall address on VDOM-A in the GUI:

1. Connect to VDOM-A.
2. Go to **Policy & Objects > Addresses** and create a new address.

**3. Enter the following information:**

|                                   |                  |
|-----------------------------------|------------------|
| <b>Address Name</b>               | FTP-server       |
| <b>Type</b>                       | Subnet           |
| <b>Subnet / IP Range</b>          | 192.168.20.10/32 |
| <b>Interface</b>                  | VDOM-link0       |
| <b>Show in Address List</b>       | enabled          |
| <b>Static Route Configuration</b> | enabled          |

**To add the firewall addresses on VDOM-A with the CLI:**

```
config vdom
 edit VDOM-B
 config firewall address
 edit FTP-server
 set associated-interface VDOM-link0
 set allow-routing enable
 set subnet 192.168.20.10 255.255.255.255
 next
 end
 next
end
```

**To add the static route on VDOM-A in the GUI:**

1. Connect to VDOM-A.
2. Go to **Network > Static Routes** and create a new route.
3. Enter the following information:

|                      |               |
|----------------------|---------------|
| <b>Destination</b>   | Named Address |
| <b>Named Address</b> | FTP-server    |
| <b>Gateway</b>       | 0.0.0.0       |
| <b>Interface</b>     | VDOM-link0    |

**To add the static route on VDOM-A with the CLI:**

```
config vdom
 edit VDOM-A
 config router static
 edit 0
 set device VDOM-link0
 set dstaddr FTP-server
 next
 end
 next
end
```

### To add the security policy on VDOM-A in the GUI:

1. Connect to VDOM-A.
2. Go to **Policy & Objects > IPv4 Policy** and create a new policy.
3. Enter the following information:

|                           |                   |
|---------------------------|-------------------|
| <b>Name</b>               | Access-FTP-server |
| <b>Incoming Interface</b> | port1             |
| <b>Outgoing Interface</b> | VDOM-link0        |
| <b>Source</b>             | internal-network  |
| <b>Destination</b>        | FTP-server        |
| <b>Schedule</b>           | always            |
| <b>Service</b>            | FTP               |
| <b>Action</b>             | ACCEPT            |
| <b>NAT</b>                | disabled          |

### To add the security policy on VDOM-A with the CLI:

```
config vdom
 edit VDOM-A
 config firewall policy
 edit 0
 set name Access-FTP-server
 set srcintf port1
 set dstintf VDOM-link0
 set srcaddr internal-network
 set dstaddr FTP-server
 set action accept
 set schedule always
 set service FTP
 next
 end
 next
end
```

### To add the firewall address on VDOM-B in the GUI:

1. Connect to VDOM-B.
2. Go to **Policy & Objects > Addresses** and create a new address.
3. Enter the following information:

|                          |                  |
|--------------------------|------------------|
| <b>Address Name</b>      | internal-network |
| <b>Type</b>              | Subnet           |
| <b>Subnet / IP Range</b> | 192.168.10.0/24  |
| <b>Interface</b>         | VDOM-link1       |

|                            |         |
|----------------------------|---------|
| Show in Address List       | enabled |
| Static Route Configuration | enabled |

### To add the firewall addresses on VDOM-B with the CLI:

```
config vdom
 edit VDOM-B
 config firewall address
 edit internal-network
 set associated-interface VDOM-link1
 set allow-routing enable
 set subnet 192.168.10.0 255.255.255.0
 next
 end
 next
end
```

### To add the static route on VDOM-B in the GUI:

1. Connect to VDOM-B.
2. Go to **Network > Static Routes** and create a new route.
3. Enter the following information:

|               |                  |
|---------------|------------------|
| Destination   | Named Address    |
| Named Address | internal-network |
| Gateway       | 0.0.0.0          |
| Interface     | VDOM-link1       |

### To add the static route on VDOM-B with the CLI:

```
config vdom
 edit VDOM-B
 config router static
 edit 0
 set device VDOM-link1
 set dstaddr internal-network
 next
 end
 next
end
```

### To add the security policy on VDOM-B in the GUI:

1. Connect to VDOM-B.
2. Go to **Policy & Objects > IPv4 Policy** and create a new policy.
3. Enter the following information:

|      |                        |
|------|------------------------|
| Name | Internal-server-access |
|------|------------------------|



|                           |                  |
|---------------------------|------------------|
| <b>Incoming Interface</b> | VDOM-link1       |
| <b>Outgoing Interface</b> | port2            |
| <b>Source</b>             | internal-network |
| <b>Destination</b>        | FTP-server       |
| <b>Schedule</b>           | always           |
| <b>Service</b>            | FTP              |
| <b>Action</b>             | ACCEPT           |
| <b>NAT</b>                | disabled         |

**To add the security policy on VDOM-B with the CLI:**

```
config vdom
 edit VDOM-B
 config firewall policy
 edit 0
 set name Internal-server-access
 set srcintf VDOM-link1
 set dstintf port2
 set srcaddr internal-network
 set dstaddr FTP-server
 set action accept
 set schedule always
 set service FTP
 next
 end
 next
end
```

## NAT and transparent mode

In this example, VDOM-A uses NAT mode and VDOM-B uses transparent mode.

This configuration requires the following steps:

1. [Configure VDOM-A on page 667](#)
2. [Configure VDOM-B on page 669](#)

## Configure VDOM-A

VDOM-A allows connections from devices on the internal network to the Internet. WAN 1 and port 1 are assigned to this VDOM.

The per-VDOM configuration for VDOM-A includes the following:

- A firewall address for the internal network
- A static route to the ISP gateway
- A security policy allowing the internal network to access the Internet

All procedures in this section require you to connect to VDOM-A, either using a global or per-VDOM administrator account.

### To add the firewall addresses in the GUI:

1. Go to *Policy & Objects > Addresses* and create a new address.
2. Enter the following information:

|                             |                  |
|-----------------------------|------------------|
| <b>Name</b>                 | internal-network |
| <b>Type</b>                 | Subnet           |
| <b>Subnet / IP Range</b>    | 192.168.10.0/24  |
| <b>Interface</b>            | port1            |
| <b>Show in Address List</b> | enabled          |

### To add the firewall addresses with the CLI:

```
config vdom
 edit VDOM-A
 config firewall address
 edit internal-network
 set associated-interface port1
 set subnet 192.168.10.0 255.255.255.0
 next
 end
 next
end
```

### To add a default route in the GUI:

1. Go to *Network > Static Routes* and create a new route.
2. Enter the following information:

|                    |                 |
|--------------------|-----------------|
| <b>Destination</b> | Subnet          |
| <b>IP address</b>  | 0.0.0.0/0.0.0.0 |
| <b>Gateway</b>     | 172.20.201.7    |
| <b>Interface</b>   | wan1            |
| <b>Distance</b>    | 10              |

### To add a default route with the CLI:

```
config vdom
 edit VDOM-A
 config router static
 edit 0
 set gateway 172.20.201.7
 set device wan1
 next
 end
 next
end
```

```
end
```

### To add the security policy in the GUI:

1. Connect to VDOM-A.
2. Go to *Policy & Objects > IPv4 Policy* and create a new policy.
3. Enter the following information:

|                            |                  |
|----------------------------|------------------|
| <b>Name</b>                | VDOM-A-Internet  |
| <b>Incoming Interface</b>  | port1            |
| <b>Outgoing Interface</b>  | wan1             |
| <b>Source Address</b>      | internal-network |
| <b>Destination Address</b> | all              |
| <b>Schedule</b>            | always           |
| <b>Service</b>             | ALL              |
| <b>Action</b>              | ACCEPT           |
| <b>NAT</b>                 | enabled          |

### To add the security policy with the CLI:

```
config vdom
 edit VDOM-A
 config firewall policy
 edit 0
 set name VDOM-A-Internet
 set srcintf port1
 set dstintf wan1
 set srcaddr internal-network
 set dstaddr all
 set action accept
 set schedule always
 set service ALL
 set nat enable
 next
 end
 next
end
```

## Configure VDOM-B

VDOM-B allows external connections to reach an internal FTP server. WAN 2 and port 2 are assigned to this VDOM.

The per-VDOM configuration for VDOM-B includes the following:

- A firewall address for the FTP server
- A static route to the ISP gateway
- A security policy allowing external traffic to reach the FTP server

All procedures in this section require you to connect to VDOM-B, either using a global or per-VDOM administrator account.

### To add the firewall addresses in the GUI:

1. Go to *Policy & Objects > Addresses* and create a new address.
2. Enter the following information:

|                             |                  |
|-----------------------------|------------------|
| <b>Address Name</b>         | FTP-server       |
| <b>Type</b>                 | Subnet           |
| <b>Subnet / IP Range</b>    | 172.25.177.42/32 |
| <b>Interface</b>            | port2            |
| <b>Show in Address List</b> | enabled          |

### To add the firewall addresses with the CLI:

```
config vdom
 edit VDOM-B
 config firewall address
 edit FTP-server
 set associated-interface port2
 set subnet 172.25.177.42 255.255.255.255
 next
 end
 next
end
```

### To add a default route in the GUI:

1. Go to *Network > Routing Table* and create a new route.
2. Enter the following information:

|                    |                 |
|--------------------|-----------------|
| <b>Destination</b> | Subnet          |
| <b>IP address</b>  | 0.0.0.0/0.0.0.0 |
| <b>Gateway</b>     | 172.20.10.10    |

### To add a default route with the CLI:

```
config vdom
 edit VDOM-B
 config router static
 edit 0
 set gateway 172.20.10.10
 next
 end
 next
end
```

**To add the security policy in the GUI:**

1. Connect to VDOM-B.
2. Go to *Policy & Objects > IPv4 Policy* and create a new policy.
3. Enter the following information:

|                            |               |
|----------------------------|---------------|
| <b>Name</b>                | Access-server |
| <b>Incoming Interface</b>  | wan2          |
| <b>Outgoing Interface</b>  | port2         |
| <b>Source Address</b>      | all           |
| <b>Destination Address</b> | FTP-server    |
| <b>Schedule</b>            | always        |
| <b>Service</b>             | FTP           |
| <b>Action</b>              | ACCEPT        |

**To add the security policy with the CLI:**

```
config vdom
 edit VDOM-B
 config firewall policy
 edit 0
 set name Access-server
 set srcintf wan2
 set dstintf port2
 set srcaddr all
 set dstaddr FTP-server-VIP
 set action accept
 set schedule always
 set service FTP
 next
 end
 next
end
```

## High Availability

The following sections provide instructions on configuring High Availability (HA):

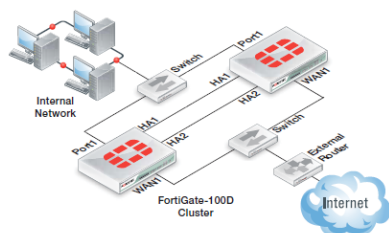
- [Introduction to the FGCP cluster on page 672](#)
- [Failover protection on page 673](#)
- [HA heartbeat interface on page 674](#)
- [FGSP \(session synchronization\) peer setup on page 683](#)
- [Synchronizing sessions between FGCP clusters on page 684](#)
- [Firmware upgrades in FGSP on page 685](#)
- [Using standalone configuration synchronization on page 686](#)
- [Troubleshoot an HA formation on page 687](#)

- [Check HA sync status on page 688](#)
- [Disabling stateful SCTP inspection on page 690](#)
- [Upgrading FortiGates in an HA cluster on page 691](#)
- [HA cluster setup examples on page 698](#)
- [Out-of-band management with reserved management interfaces on page 692](#)
- [In-band management on page 697](#)

## Introduction to the FGCP cluster

High availability (HA) is usually required in a system where there is high demand for little downtime. There are usually hot-swaps, backup routes, or standby backup units and as soon as the active entity fails, backup entities will start functioning. This results in minimal interruption for the users.

The FortiGate Clustering Protocol (FGCP) is a proprietary HA solution whereby FortiGates can find other member FortiGates to negotiate and create a cluster. A FortiGate HA cluster consists of at least two FortiGates (members) configured for HA operation. All FortiGates in the cluster must be the same model and have the same firmware installed. Cluster members must also have the same hardware configuration (such as the same number of hard disks). All cluster members share the same configurations except for their host name and priority in the HA settings. The cluster works like a device but always has a hot backup device.



## Critical cluster components

The following are critical components in an HA cluster:

- Heartbeat connections: members will use this to communicate with each other. In general, a two-member cluster is most common. We recommend double back-to-back heartbeat connections.
- Identical connections for internal and external interfaces: as demonstrated in the topology, we recommend similar connections from each member to the switches for the cluster to function properly.

## General operation

The following are best practices for general cluster operation:

- Ensure that heartbeat communication is present (see [HA heartbeat interface on page 674](#)).
- Enable the session synchronization option in daily operation (see [FGSP \(session synchronization\) peer setup on page 683](#)).
- Monitor traffic flowing in and out of the interfaces.

## Failover

FGCP provides failover protection in the following scenarios:

- The active device loses power.
- A monitored interface loses a connection.

After failover occurs, the user will not notice any difference, except that the active device has changed. See [Failover protection on page 673](#) for more information.

## Synchronizing the configuration

FGCP uses a combination of incremental and periodic synchronization to make sure that the configuration of all cluster units is synchronized to that of the primary unit.

The following settings are not synchronized between cluster units:

- The FortiGate host name
- GUI Dashboard widgets
- HA override
- HA device priority
- The virtual cluster priority
- The HA priority setting for a ping server (or dead gateway detection) configuration
- The system interface settings of the HA reserved management interface
- The HA default route for the reserved management interface, set using the `ha-mgmt-interface-gateway` option of the `config system ha` command

Most subscriptions and licenses are not synchronized, as each FortiGate must be licensed individually. FortiToken Mobile is an exception; they are registered to the primary unit and synchronized to the secondary units.

The primary unit synchronizes all other configuration settings, including the other HA configuration settings.

All synchronization activity takes place over the HA heartbeat link using TCP/703 and UDP/703 packets.

## Failover protection

The FortiGate Clustering Protocol (FGCP) provides failover protection, meaning that a cluster can provide FortiGate services even when one of the devices in the cluster encounters a problem that would result in the complete loss of connectivity for a stand-alone FortiGate unit. Failover protection provides a backup mechanism that can be used to reduce the risk of unexpected downtime, especially in mission-critical environments.

FGCP supports failover protection in three ways:

1. Link failover maintains traffic flow if a link fails.
2. If a device loses power, it automatically fails over to a backup unit with minimal impact on the network.
3. Optionally, if an SSD fails, it can automatically fail over to a backup unit.

When session-pickup is enabled in the HA settings, existing TCP sessions are kept, and users on the network are not impacted by downtime as the traffic can be passed without reestablishing the sessions.

## When and how the failover happens

### 1. Link fails

Before triggering a failover when a link fails, the administrator must ensure that monitor interfaces are configured.

Normally, the internal interface that connects to the internal network, and an outgoing interface for traffic to the internet or outside the network, should be monitored. Any of those links going down will trigger a failover.

## 2. Loss of power for active unit.

When an active (primary) unit loses power, a backup (secondary) unit automatically becomes the primary, and the impact on traffic is minimal. There are no settings for this kind of fail over.

## 3. SSD failure

HA failover can be triggered by an SSD failure.

### To enable an SSD failure triggering HA fail over:

```
config system ha
 set ssd-failover enable
end
```

## HA heartbeat interface

The HA heartbeat allows cluster units to communicate with each other. The heartbeat consists of hello packets that are sent at regular intervals by the heartbeat interface of all cluster units. The hello packets describe the state of the cluster unit (including communication sessions) and are used by other cluster units to keep the cluster synchronized. While the cluster is operating, the HA heartbeat confirms that all cluster units are functioning normally.

HA heartbeat packets are Layer 2 Ethernet frames that use EtherType values of 0x8890 and 0x8891 rather than 0x0800 for normal 802.3 IP packets. The default time interval between HA heartbeats is 200 ms.

As a best practice, it is recommended to isolate the heartbeat devices from the user networks by connecting the heartbeat devices to a dedicated switch that is not connected to any network. The heartbeat packets contain sensitive information about the cluster configuration and may use a considerable amount of network bandwidth. If the cluster consists of two FortiGates, connect the heartbeat device interfaces back-to-back using a crossover cable. If there are more than two FortiGates, each heartbeat interface should be connected to a dedicated switch. For example, in a four-member HA cluster with two heartbeat interfaces, there would be two switches (one switch dedicated to each interface).

Upon starting up, a FortiGate configured for HA broadcasts HA heartbeat hello packets from its HA heartbeat interface to find other FortiGates configured to operate in HA mode. If two or more FortiGates operating in HA mode connect with each other, they compare HA configurations (mode, password, and group ID). If the HA configurations match, then the units negotiate to form a cluster.

## Configuring an HA heartbeat interface

A heartbeat interface is an Ethernet network interface in a cluster that is used by the FGCP for HA heartbeat communications between cluster units.

By default, two interfaces are configured to be heartbeat interfaces on most FortiGate models. The heartbeat interface configuration can be changed to select an additional or different heartbeat interface. It is possible to select only one heartbeat interface; however, this is not a recommended configuration (see [Split brain scenario on page 675](#)).

Another important setting in the HA configuration is the heartbeat interface priority. In all cases, the heartbeat interface with the highest priority is used for all HA heartbeat communication. If the interface fails or becomes disconnected, then the selected heartbeat interface with the next highest priority handles all HA heartbeat communication.

If more than one heartbeat interface has the same priority, the heartbeat interface with the highest priority that is also highest in the heartbeat interface list is used for all HA heartbeat communication. If this interface fails or becomes



disconnected, then the selected heartbeat interface with the highest priority that is next highest in the list handles all heartbeat communication (see [Selecting heartbeat packets and interfaces on page 676](#)).

The default heartbeat interface configuration sets the priority of both heartbeat interfaces to 50, and the range is 0 to 512. When selecting a new heartbeat interface, the default priority is 0. The higher the number, the higher the priority.

In most cases, the default heartbeat interface configuration can be maintained as long the heartbeat interfaces are connected. Configuring HA heartbeat interfaces is the same for virtual clustering and for standard HA clustering. Up to eight heartbeat interface can be selected. This limit only applies to FortiGates with more than eight physical interfaces.



Heartbeat communications can be enabled on physical interfaces, but not on switch ports, VLAN subinterfaces, IPsec VPN interfaces, redundant interfaces, or 802.3ad aggregate interfaces.

---

### To change the heartbeat interfaces in the GUI:

1. Go to *System > HA* and select a *Mode*.
2. Click the + in the *Heartbeat interfaces* field to select an interface.
3. Click *OK*.

### To configure two interfaces as heartbeat interfaces with the same priority in the CLI:

```
config system ha
 set hbdev port4 150 port5 150
end
```

In this example, port4 and port5 are configured as the HA heartbeat interfaces and they both have a priority of 150.

### To configure two interfaces as heartbeat interfaces with different priorities in the CLI:

```
config system ha
 set hbdev port4 100 port1 50
end
```

In this example, port4 and port1 are configured as the HA heartbeat interfaces. The priority for port4 is higher (100) than port1 (50), so port4 is the preferred HA heartbeat interface.

## Split brain scenario

At least one heartbeat interface must be selected for the HA cluster to function correctly. This interface must be connected to all the units in the cluster. If heartbeat communication is interrupted and cannot fail over to a second heartbeat interface, then the cluster units will not be able to communicate with each other and more than one cluster unit may become a primary unit. As a result, the cluster stops functioning normally because multiple devices on the network may be operating as primary units with the same IP and MAC addresses creating a split brain scenario. See [Split brain scenario: on page 688](#) for more information.

## Sharing heartbeat interfaces with traffic ports

HA heartbeat and data traffic is supported on the same cluster interface. In NAT mode, if the heartbeat interfaces are used for processing network traffic, then the interface can be assigned any IP address. The IP address does not affect HA heartbeat traffic.

In transparent mode, the heartbeat interface can be connected to the network with management access enabled on the same interface. A management connection would then be established to the interface using the transparent mode management IP address. This configuration does not affect HA heartbeat traffic.

While these configurations are allowable, they are not recommended. When possible, use dedicated interfaces for heartbeat traffic.

## Selecting heartbeat packets and interfaces

HA heartbeat hello packets are sent constantly by all of the enabled heartbeat interfaces. Using these hello packets, each cluster unit confirms that the other cluster units are still operating. The FGCP selects one of the heartbeat interfaces to be used for communication between the cluster units. This interface is used for heartbeat communication and is based on the linkfail states of the heartbeat interfaces, the heartbeat interface priority, and the interface index. The connected heartbeat interface with the highest priority is selected for heartbeat communication.

If more than one connected heartbeat interface has the highest priority, then the FGCP selects the heartbeat interface with the lowest interface index. The interface index order is visible in the CLI by running the `diagnose netlink interface list` command.

If the interface that is processing heartbeat traffic fails or becomes disconnected, the FGCP uses the same criteria to select another heartbeat interface for heartbeat communication. If the original heartbeat interface is fixed or reconnected, the FGCP selects this interface again for heartbeat communication.

The HA heartbeat interface communicates cluster session information, synchronizes the cluster configuration, synchronizes the cluster kernel routing table, and reports individual cluster member statuses. The HA heartbeat constantly communicates HA status information to make sure that the cluster is operating properly.

## Modifying heartbeat timing

The heartbeat interval and heartbeat lost threshold are two variables that dictate the length of time one cluster unit will wait before determining a peer is dead.

```
config system ha
 set hb-interval <integer>
 set hb-interval-in-milliseconds {100 | 10}
 set hb-lost-threshold <integer>
end
```

|                                                     |                                                                                                                   |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <code>hb-interval &lt;integer&gt;</code>            | Set the time between sending heartbeat packets; increase to reduce false positives (1 - 20, default = 2).         |
| <code>hb-interval-in-milliseconds {100   10}</code> | Set the number of milliseconds for each heartbeat interval (100 or 10, default = 100).                            |
| <code>hb-lost-threshold &lt;integer&gt;</code>      | Set the number of lost heartbeats to signal a failure; increase to reduce false positives (1 - 60, default = 20). |

Heartbeats are sent out every  $2 \times 100$  ms, and it takes 20 consecutive lost heartbeats for a cluster member to be detected as dead. Therefore, it takes by default  $2 \times 100 \text{ ms} \times 20 = 4000 \text{ ms}$ , or 4 seconds, for a failure to be detected.

Sub-second heartbeat failure detection can be achieved by lowering the interval and threshold or lowering the heartbeat interval unit of measurement from 100 ms to 10 ms.

If the primary unit does not receive a heartbeat packet from a subordinate unit before the heartbeat threshold expires, the primary unit assumes that the subordinate unit has failed.

If a subordinate unit does not receive a heartbeat packet from the primary unit before the heartbeat threshold expires, the subordinate unit assumes that the primary unit has failed. The subordinate unit then begins negotiating to become the new primary unit.

The HA heartbeat packets consume more bandwidth if the heartbeat interval is short. But if the heartbeat interval is very long, the cluster is not as sensitive to topology and other network changes. Therefore, gauge your settings based on the amount of traffic and CPU usage sustainable by the cluster units versus the tolerance for an outage when the primary unit fails. Avoid using the heartbeat interfaces as traffic ports to prevent congesting the interfaces.

## Changing the time to wait in the hello state

The hello state hold down time is the number of seconds that a cluster unit waits before changing from hello state to work state. After a failure or when starting up, cluster units operate in the hello state to send and receive heartbeat packets so that all the cluster units can find each other and form a cluster. A cluster unit should change from the hello state to work state after it finds all the other FortiGate units to form a cluster with.

If all cluster units cannot find each other during the hello state, then some cluster units may join the cluster after it has formed. This can cause disruptions to the cluster and affect how it operates. A delay could occur if the cluster units are located at different sites or if communication is delayed between the heartbeat interfaces. If delays occur, increase the cluster units wait time in the hello state.

```
config system ha
 set hello-holddown <integer>
end
```

|                                             |                                                                                                    |
|---------------------------------------------|----------------------------------------------------------------------------------------------------|
| <code>hello-holddown &lt;integer&gt;</code> | Set the time to wait before changing from hello to work state, in seconds (5 - 300, default = 20). |
|---------------------------------------------|----------------------------------------------------------------------------------------------------|

## Configuring HA heartbeat encryption and authentication

HA heartbeat encryption and authentication to encrypt and authenticate HA heartbeat packets can be enabled. HA heartbeat packets should be encrypted and authenticated if the cluster interfaces that send HA heartbeat packets are also connected to the networks. HA heartbeat encryption and authentication are disabled by default. Note that enabling these settings could reduce cluster performance.

```
config system ha
 set authentication {enable | disable}
 set encryption {enable | disable}
end
```

If HA heartbeat packets are not encrypted, the cluster password and changes to the cluster configuration could be exposed. An attacker may be able to sniff HA packets to get cluster information. Enabling HA heartbeat message authentication prevents an attacker from creating false HA heartbeat messages. False HA heartbeat messages could affect the stability of the cluster.

HA authentication and encryption uses AES-128 for encryption and SHA1 for authentication. Heartbeat messages are encrypted and encapsulated in ESP packets for transfer in an IPsec tunnel between the cluster members.

## Heartbeat bandwidth requirements

The majority of the traffic processed by the HA heartbeat interface is session synchronization traffic. Other heartbeat interface traffic required to synchronize IPsec states, IPsec keys, routing tables, configuration changes, and so on is usually negligible.

The amount of traffic required for session synchronization depends on the connections per second (CPS) that the cluster is processing, since only new sessions (and session table updates) need to be synchronized.

Another factor to consider is that if session pickup is enabled, the traffic on the heartbeat interface surges during a failover or when a unit joins or re-joins the cluster. When one of these events occurs, the entire session table needs to be synchronized. Lower throughput HA heartbeat interfaces may increase failover time if they cannot handle the higher demand during these events.

The amount of heartbeat traffic can also be reduced by:

- Turning off session pickup if it is not needed
- Enabling `session-pickup-delay` to reduce the number of sessions that are synchronized
- Using the `session-sync-dev` option to move session synchronization traffic off of the heartbeat link

## Heartbeat packet EtherTypes

Normal 802.3 IP packets have an EtherType field value of 0x0800. EtherType values other than 0x0800 are understood as Layer 2 frames rather than IP packets.

HA heartbeat packets use the following EtherTypes:

| Field value | Function                                           | Description                                                                                                                                                                                                                                                                |
|-------------|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0x8890      | Heartbeat                                          | Heartbeat packets are used by cluster units to find other cluster units, and to verify the status of other cluster units while the cluster is operating.<br>Use the <code>ha-eth-type</code> option to change the EtherType.                                               |
| 0x8891      | Traffic redistribution from primary to subordinate | These are used when the HA primary needs to redistribute traffic packets and the corresponding session information to the subordinate units in A-A mode.<br>Use the <code>hc-eth-type</code> option to change the EtherType.                                               |
| 0x8892      | Session synchronization                            | Session synchronization uses the heartbeat interfaces for communication, unless session synchronization devices are specified. See <a href="#">Session synchronization on page 679</a> for more information.                                                               |
| 0x8893      | HA Telnet sessions (configuration synchronization) | The Telnet sessions are used to synchronize the cluster configurations, and to connect from one cluster unit's CLI to another when an administrator uses the <code>execute ha manage</code> command.<br>Use the <code>l2ep-eth-type</code> option to change the EtherType. |

## Session synchronization

Since large amounts of session synchronization traffic can increase network congestion, it is recommended to keep this traffic off of the network and separate from the HA heartbeat interfaces by using dedicated connections for it. The interfaces are configured in the `session-sync-dev` setting.

The session synchronization device interfaces must be connected together by directly using the appropriate cable or using switches. If one of the interfaces becomes disconnected, then the cluster uses the remaining interfaces for session synchronization. If all the session synchronization interfaces become disconnected, then session synchronization reverts to using the HA heartbeat link.

All session synchronization traffic is between the primary unit and each subordinate unit. Session synchronization always uses UDP/708, but this will be encapsulated differently depending on the `session-sync-dev` setting. If `session-sync-dev` is specified, the packets will use 0x8892 and will exit over the mentioned port. If `session-sync-dev` is not specified, the packets will use 0x8893 and will exit the heartbeat port.

Session synchronization packets are typically processed by a single CPU core because all source and destination MAC addresses of the L2 frames are the same. Hashing based on the L2 addresses maps the processing of the frames to the same core. When large amounts of session synchronization traffic must be processed, enable the `sync-packet-balance` setting to distribute the processing to more cores. This effectively uses a larger set of MAC addresses for the hashing to map to multiple cores.

## Troubleshooting heartbeat packets

Understanding the different types of heartbeat packets will ease troubleshooting. Heartbeat packets are recognized as Layer 2 frames. The switches and routers on the heartbeat network that connect to heartbeat interfaces must be configured to allow them to pass through. If Layer 2 frames are dropped by these network devices, then the heartbeat traffic will not be allowed between the cluster units.

For example, some third-party network equipment may not allow EtherType 0x8893. The unit can still be found in the HA cluster, but you would be unable to run `execute ha manage` to manage the other unit. Use the following settings to change the EtherTypes of the HA heartbeat packets, if they require changing them for the traffic to be forwarded on the connected switch.

```
config system ha
 set ha-eth-type <hex_value>
 set hc-eth-type <hex_value>
 set l2ep-eth-type <hex_value>
end
```

### To change the EtherType values of the heartbeat and HA Telnet session packets:

```
config system ha
 set ha-eth-type 8895
 set l2ep-eth-type 889f
end
```

For troubleshooting issues with packets sent or received on the HA heartbeat ports, use the following diagnostic command to sniff the traffic by EtherType.

```
diagnose sniffer packet any 'ether proto <EtherType_in_hex>' 6 0 1
```

**To sniff the traffic on EtherType 0x8890:**

```
diagnose sniffer packet any 'ether proto 0x8890' 6 0 1
Using Original Sniffing Mode
interfaces=[any]
filters=[ether proto 0x8890]
2022-10-19 16:22:26.512813 port5 out Ether type 0x8890 printer hasn't been added to sniffer.
0x0000 0000 0000 0000 000c 293b e61c 8890 5201 );....R.
0x0010 020c 6e65 7700 0000 0000 0000 0000 0000 ..new.....
0x0020 0000 0000 0000 0000 0000 0000 0000 0000
0x0030 0000 0000 0700 0000 0000 0000 0000 8738 8
0x0040 0100 706f 7274 3500 0000 0000 0000 0000 ..port5.....
0x0050 0000 0300 843d 4647 564d 3034 544d 3232 =FGVM04TM22
0x0060 3030 3236 3338 0b00 0100 000c 0001 00c8 002001.....
0x0070 0d00 0100 000e 0004 0009 0000 000f 0004
0x0080 0000 0000 0010 0004 0000 0000 0011 0004
0x0090 0000 0000 0012 0004 0001 0000 0028 0000 (..
0x00a0 002b 0002 000a 002c 0002 000a 0038 0008 .+.....,.....8..
0x00b0 00c0 0300 0000 0000 0037 0004 0000 0000 7.....
0x00c0 003c 0030 0030 2704 175f 0858 9d4f 5611 .<.0.0'.._X.OV.
0x00d0 2005 6310 b1b0 be14 e029 1f5b 61fd 5b49 ..c.....).[a.[I
0x00e0 7cad bed4 ecaf 05bd 70c3 2adc 4fa0 6ab7 |.....p.*.O.j.
0x00f0 4d5d 1df7 4f3d 000c 0007 0000 0002 0000 M]..O=.....
0x0100 0085 0400 003e 0001 0000 4000 0400 0000 >....@.....
0x0110 0000 3f00 2400 0000 0000 0000 0000 0000 ..?.$.....
0x0120 0000 0000 0000 0000 0000 0000 0000 0000
0x0130 0000 0000 0000 0000 0000 3300 0400 0000 3.....
0x0140 0000 2a00 7200 0a00 789c edcc 290e c250 ..*.r...x...)..P
0x0150 1440 d19f d420 5068 3449 5dc8 d009 8b66 .@....Ph4I]....f
0x0160 2b34 8435 b302 3401 9e22 6f05 15e7 c82b +4.5..4.."o....+
0x0170 ee7c bb3f daf2 675d 9f9f af6a fee6 7dce .|.?.g]...j..}.
0x0180 efc8 879c 5791 8f39 6f22 9f72 de46 ee72 W..9o".r.F.r
0x0190 de45 ee73 6eca 2f0f 394f 91c7 9c2f 3169 .E.sn./90.../li
0x01a0 9b94 af55 0100 0000 0000 0000 0000 0000 ...U.....
0x01b0 0058 ac0f 0096 24af 0000 0000 .X....$.....

2022-10-19 16:22:26.545236 port5 in Ether type 0x8890 printer hasn't been added to sniffer.
0x0000 ffff ffff ffff 000c 29ca ba5d 8890 5201 )]..R.
0x0010 020c 6e65 7700 0000 0000 0000 0000 0000 ..new.....
0x0020 0000 0000 0000 0000 0000 0000 0000 0000
0x0030 0000 0000 0700 0000 0000 0000 0000 8738 8
0x0040 0100 706f 7274 3500 0000 0000 0000 0000 ..port5.....
0x0050 0000 0300 d221 4647 564d 3034 544d 3232 !FGVM04TM22
0x0060 3030 3236 3339 0b00 0100 000c 0001 0080 002002.....
0x0070 0d00 0100 000e 0004 0000 0000 000f 0004
0x0080 0000 0000 0010 0004 0000 0000 0011 0004
0x0090 0000 0000 0012 0004 0000 0000 0028 0000 (..
0x00a0 002b 0002 000a 002c 0002 000a 0038 0008 .+.....,.....8..
0x00b0 00e6 0400 0000 0000 0037 0004 0000 0000 7.....
0x00c0 003c 0030 0029 6d7e 3407 2d31 c00f 42b3 .<.0.)m~4.-1..B.
0x00d0 59b6 17cb 4be7 d043 a158 e74c 5841 c821 Y...K..C.X.LXA.!
0x00e0 7843 b598 c95d 3dcf 81a9 bc8b b304 53f3 xC...]=.....S.
0x00f0 17b6 3cd5 a83d 000c 0007 0000 0002 0000 ..<..=.....
0x0100 0085 0400 0040 0004 0000 0000 003f 0024 @.....?.$
0x0110 0000 0000 0000 0000 0000 0000 0000 0000
0x0120 0000 0000 0000 0000 0000 0000 0000 0000
```

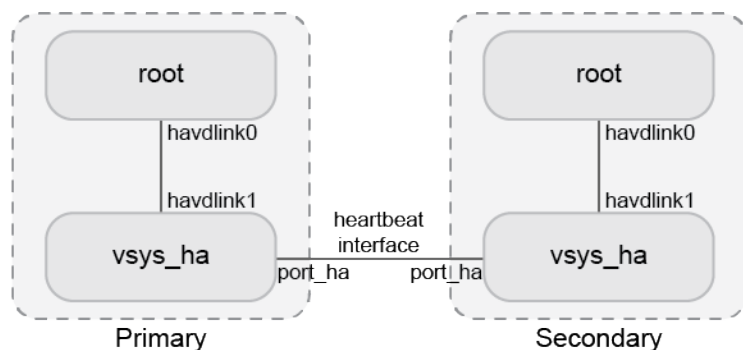
```

0x0130 0000 0000 0033 0004 0000 0000 002a 0073 3.....*.s
0x0140 000a 0078 9ced cc21 1282 5014 40d1 3f43 ...x...!...P.@.?C
0x0150 7523 3651 414c 66b2 994c 1419 9bd9 ec7e u#6QALf..L.....~
0x0160 5c82 ab52 5e72 de0a 0ce7 c41b ee74 996f \..R^r.....t.o
0x0170 75f9 b15a bf5f 4d35 7df3 36e7 53e4 5dce u..Z._M5}.6.S.].
0x0180 7de4 7dce e7c8 4dce 43e4 36e7 31f2 21e7 }.}...M.C.6.1.!.
0x0190 6b59 7297 f33d f231 e747 4cea 4dca cfaa kYr..=.1.GL.M...
0x01a0 0000 0000 0000 0000 0000 0000 00fc ad0f
0x01b0 c16c 2917 0000 0000 .l).....

```

## Interface IP addresses

An FGCP cluster communicates heartbeat packets using Layer 2 frames over the physical heartbeat interface, but it also communicates other synchronization traffic, logs, and locally generated traffic from subordinate devices over Layer 3 IP packets. Additional virtual interfaces are created in the hidden vsys\_ha VDOM, which need to be addressed with IPv4 addresses.



The FGCP uses link-local IPv4 addresses (see [RFC 3927](#)) in the 169.254.0.x range for the virtual HA heartbeat interface (port\_ha) and for the inter-VDOM link interfaces between the vsys\_ha and management VDOM. When members join an HA cluster, each member's heartbeat interface (port\_ha) is assigned an IP address from the range of 169.254.0.1 to 169.254.0.63/26. HA inter-VDOM link interfaces (havdlink0 and havdlink1) are assigned IP address from the range of 169.254.0.65 to 169.254.0.66/26.

The IP address that is assigned to a virtual heartbeat interface depends on the serial number priority of the member. Higher serial numbers have a higher priority, and therefore a lower serialno\_prio number, for example:

```

diagnose sys ha status
...
FGVM08TM20002002: Secondary, serialno_prio=0, usr_priority=128, hostname=FGVM08TM20002002
FGVM08TM19003001: Primary, serialno_prio=1, usr_priority=128, hostname=FGVM08TM19003001

```

The member with serialno\_prio=0 is assigned IP address 169.254.0.1, serialno\_prio=1 is assigned 169.254.0.2, and so forth.

### To view the HA heartbeat interface IP address of the primary unit:

```

get system ha status
...
vcluster 1: work 169.254.0.2
...

```

**To view all the assigned IP addresses of a device:**

```
diagnose ip address list
IP=172.16.151.84->172.16.151.84/255.255.255.0 index=3 devname=port1
IP=192.168.2.204->192.168.2.204/255.255.255.0 index=6 devname=port2
IP=10.10.10.1->10.10.10.1/255.255.255.0 index=9 devname=port3
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=13 devname=root
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=16 devname=vsys_ha
IP=169.254.0.2->169.254.0.2/255.255.255.192 index=17 devname=port_ha
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=18 devname=vsys_fgfm
IP=169.254.0.65->169.254.0.65/255.255.255.192 index=19 devname=havdlink0
IP=169.254.0.66->169.254.0.66/255.255.255.192 index=20 devname=havdlink1
```

When generating traffic from a subordinate unit, traffic will be routed to the primary unit's port\_ha virtual heartbeat interface. From there, if traffic is destined to another network, the traffic is routed from the vsys\_ha VDOM to the management VDOM by the havdlink interfaces.

Use the `execute traceroute` command on the subordinate unit to display HA heartbeat IP addresses and the HA inter-VDOM link IP addresses.

**To trace the route to an IP address on a subordinate unit:**

```
execute ha manage 1
execute traceroute 172.20.20.10
traceroute to 172.20.20.10 (172.20.20.10), 32 hops max, 72 byte packets
1 169.254.0.1 0 ms 0 ms 0 ms
2 169.254.0.66 0 ms 0 ms 0 ms
3 172.20.20.10 0 ms 0 ms 0 ms
```

**To run a sniffer trace on the primary unit to view the traffic flow:**

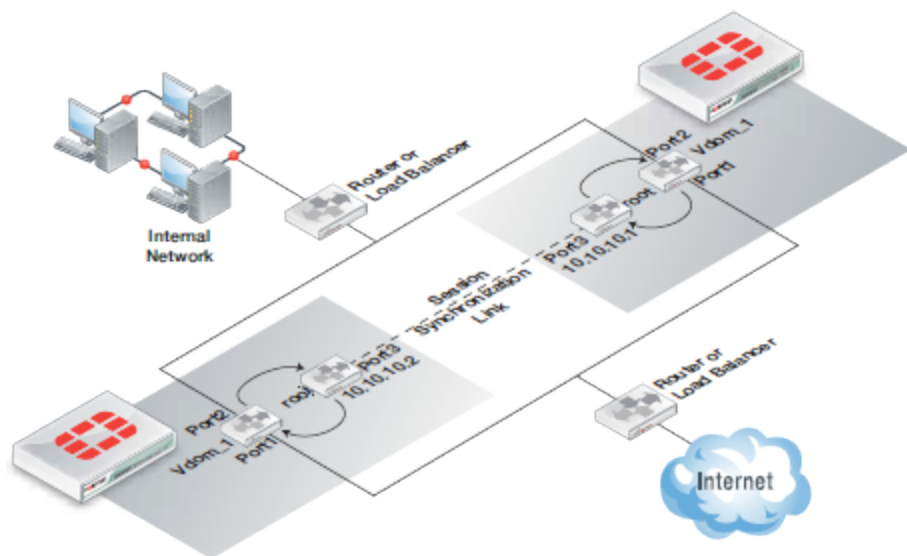
```
diagnose sniffer packet any 'net 169.254.0.0/24' 4 0 1
```



## FGSP (session synchronization) peer setup

The FortiGate Session Life Support Protocol (FGSP) is a proprietary HA solution for only sharing sessions between two entities and is based on a peer-to-peer structure. The entities could be standalone FortiGates or an FGCP cluster.

Connect all necessary interfaces as per the topology diagram below. Interfaces may be changed depending on the models in use. Interface names in the topology diagram are for example purposes only.



### To setup an FGSP peer through the CLI:

These instructions assume that the device has been connected to the console, the CLI is accessible, and that all FortiGates have been factory reset.

1. Connect all necessary interfaces as per the topology diagram.
2. Enter the following command to change the FortiGate unit host name:

```
config system global
 set hostname Example1_host(Example2_host, etc)
end
```

3. On each FGSP peer device, enter the following command:

```
config system cluster-sync
 set peerip xx.xx.xx.xx --->> peer's interface IP for session info to be
 passed.
end
```

4. Set up identical firewall policies.  
FGSP peers share the same session information which goes from the same incoming interface (example: port1) to the outgoing interface (example: port2). Firewall policies should be identical as well, and can be copied from one device to its peer.

### To test the setup:

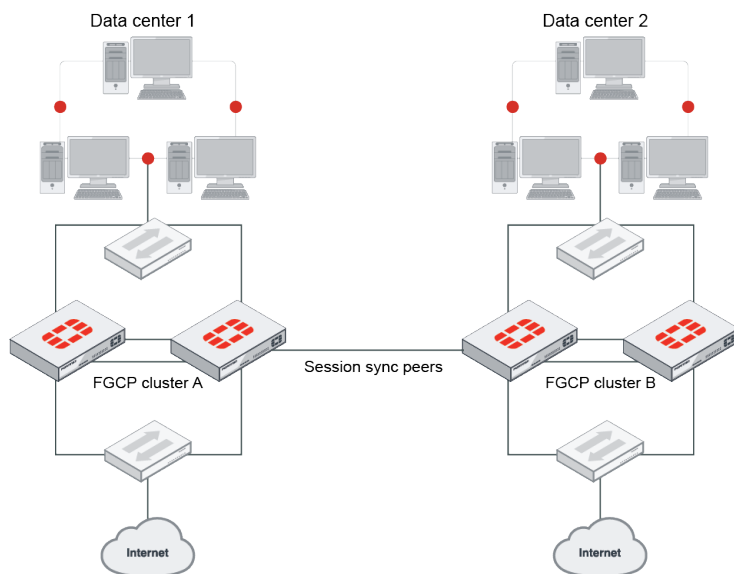
1. Initiate TCP traffic (like HTTP access) to go through *FortiGateA*.
2. Check the session information.  
For example:

```
diagnose sys session filter src xxx.xxx.xxx.xxx (your PCs IP)
diagnose sys session list
```

3. Use the same command on *FortiGateB* to determine if the same session information appeared.

## Synchronizing sessions between FGCP clusters

Synchronizing sessions between FGCP clusters is useful when data centers in different locations are used for load-balancing, and traffic must be shared and flow freely based on demand.



There are some limitations when synchronizing sessions between FGCP clusters:

- All FortiGates must have the same model and generation, hardware configuration, and FortiOS version.
- All sessions cannot be synced between clusters. Currently, only TCP sessions can be synced.
- A total of 16 clusters can share sessions.

### To configure session synchronization between two clusters:

1. Configure the two clusters (see [HA active-passive cluster setup on page 698](#) or [HA active-active cluster setup on page 700](#)).
2. On each cluster, enable session synchronization among HA clusters:

```
config system ha
 set inter-cluster-session-sync enable
end
```

3. On cluster A, configure the peer IP for the interface:

```
config system interface
 edit "port5"
 set vdom "root"
 set ip 10.10.10.1 255.255.255.0
 set allowaccess ping https ssh snmp http telnet
 next
end
```

In this example, cluster A uses port5 and its IP address, 10.10.10.1, is reachable from another cluster.

**4. On cluster A, configure cluster synchronization:**

```
config system cluster-sync
 edit 1
 set peerip 10.10.10.2
 next
end
```

**5. On cluster B, configure the peer IP for the interface:**

```
config system interface
 edit "port5"
 set vdom "root"
 set ip 10.10.10.2 255.255.255.0
 set allowaccess ping https ssh snmp http telnet
 next
end
```

In this example, cluster B uses port5 and its IP address, 10.10.10.2, is reachable from another cluster.

**6. On cluster B, configure cluster synchronization:**

```
config system cluster-sync
 edit 1
 set peerip 10.10.10.1
 next
end
```

## Firmware upgrades in FGSP

The following steps are recommended to upgrade the firmware of FortiGates in an FGSP deployment. Follow these steps whether or not you have enabled standalone configuration synchronization.

This example FGSP deployment has two FortiGates, FGT-1 and FGT-2.

**To upgrade the firmware in an FGSP deployment:**

1. Switch all traffic to FGT-1:
  - a. Configure the load balancer or router that distributes traffic between the FortiGates to send all traffic to FGT-1.
2. Disconnect FGT-2 from the network.

Make sure to also disconnect the interfaces that allow heartbeat and synchronization communication with FGT-1. This is to prevent FGT-2 from communicating with FGT-1.
3. Upgrade the firmware on FGT-2.
4. Reconnect the traffic interfaces on FGT-2, but not the interfaces used for heartbeat and synchronization communication with FGT-1.
5. Switch all traffic to the newly upgraded FGT-2:
  - a. Configure the load balancer or router that distributes traffic between the FortiGates to send all traffic to FGT-2.
6. Upgrade the firmware on FGT-1 (while heartbeat and synchronization communication with FGT-2 remains disconnected).
7. Reconnect the FGT-2 interfaces that allow heartbeat and synchronization communication between FGT-1 and FGT-2.
8. Restore the original traffic distribution between FGT-1 and FGT-2:
  - a. Configure the load balancer or router to distribute traffic to both FortiGates in the FGSP deployment.

## Using standalone configuration synchronization

You can configure synchronization from one standalone FortiGate to another standalone FortiGate (`standalone-config-sync`). With the exception of some configurations that do not sync (settings that identify the FortiGate to the network), the rest of the configurations are synced, such as firewall policies, firewall addresses, and UTM profiles.

This option is useful in situations when you need to set up FGSP peers, or when you want to quickly deploy several FortiGates with the same configurations. You can set up `standalone-config-sync` for multiple members.



`standalone-config-sync` is an independent feature and should be used with caution as there are some limitations. We recommend disabling it once the configurations have been synced over.

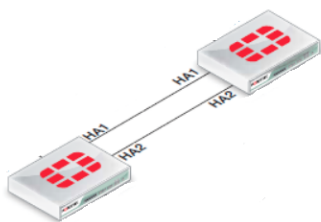
### Limitations

When standalone configuration synchronization is enabled, there are some limitations, including but not limited to the following:

- Network interruptions occur during firmware upgrades: when upgrading the firmware, all members in the `standalone-config-sync` group are upgraded simultaneously. This creates downtime if the FortiGates are the only outgoing gateway in the network. We recommend disabling the option before upgrading firmware.
- Some unwanted configurations might be synced: the current design and implementation of `standalone-config-sync` is based on requirements from specific customers. Thus, some users may find that unwanted parts of the configurations are synced. Should this occur, we recommend disabling the option and modifying those configurations manually.
- The wrong primary device might be picked accidentally: `standalone-config-sync` is derived from the HA primary unit selection mechanism. All members in the group will join the selection process in the same way as a the HA cluster selection process. It is important to select the correct device as the primary, otherwise the wrong device could be selected and existing configurations could be overwritten.
- Layer 2 heartbeat connections must be present: similar to HA heartbeat requirements, one or more layer 2 heartbeat connections are needed to sync configurations between the primary and secondary devices.

### Setting up standalone configuration synchronization

Two or more standalone FortiGates should be connected to each other with one or more heartbeat interfaces, either back-to-back or via a switch. In the following example, the device supplying the configurations is called "conf-prim," and the devices receiving the configurations are called "conf-seco".



**To set up standalone configuration synchronization:**

1. Configure the conf-prim device for the group:

```
config system ha
 set hbdev ha1 50 ha2 100
 set priority 255
 set override enable
 set standalone-config-sync enable
end
```

2. Configure the conf-prim device as needed to be functional.

3. Configure the other group members as conf-seco:

```
config system ha
 set standalone-config-sync enable
end
```

4. Wait 10–15 minutes for the configurations to sync over.

5. Verify the synchronization status:

```
get sys ha status...
Configuration Status:
 FG201E4Q17900771(updated 3 seconds ago): out-of-sync
 FG201ETK19900991(updated 1 seconds ago): in-sync
System Usage stats:
 FG201E4Q17900771(updated 3 seconds ago):
 sessions=1, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=16%
 FG201ETK19900991(updated 1 seconds ago):
 sessions=1, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=16%
...
```

If all members are `in-sync`, this means all members share the same configurations, except those that should not be synced. If any members are `out-of-sync`, this means the member failed to sync with the primary device.



Debugging is similar when a cluster is out of sync.

---

## Troubleshoot an HA formation

The following are requirements for setting up an HA cluster or FGSP peers.

Cluster members must have:

- The same model.
- The same hardware configuration.
- The same connections.
- The same generation.



The requirement to have the same generation is done as a best practice as it avoids issues that can occur later on. If you are unsure if the FortiGates are from the same generation, please contact customer service.

---

## Troubleshooting common HA formation errors

### One member keeps shutting down during HA setup (hard drive failure):

If one member has a hard drive failure but the other does not, the one with the hard drive failure will be shut down during HA setup. In this case, RMA the member to resolve the issue.

### Split brain scenario:

A split brain scenario occurs when two or more members of a cluster cannot communicate with each other on the heartbeat interface, causing each member to think it is the primary. As a result, each member assumes the primary HA role and applies the same IP and virtual MAC addresses on its interfaces. This causes IP and MAC conflicts on the network, and causes flapping on L2 devices when they learn the same MAC address on ports connected to different FortiGates.

A split brain scenario is usually caused by a complete lost of the heartbeat link or links. This can be a physical connectivity issue, or less commonly, something blocking the heartbeat packets between the HA members. Another cause is congestion and latency in the heartbeat links that exceeds the heartbeat lost intervals and thresholds.

The following are common symptoms of a split brain scenario:

- The connections to the FortiGates in the cluster work intermittently when trying to connect with administrative access.
- Sessions cannot be established through the FortiGate, and the traffic drops.
- When logging in to the FortiGates using the console, `get system ha status` shows each FortiGate as the primary.

To resolve a split brain scenario:

- Be physically on-site with the FortiGates (recommended). If this is not possible, connect to the FortiGates using console access.
- Identify the heartbeat ports, and verify that they are physically connected and up.
- Verify that heartbeat packets are being sent and received on the heartbeat ports.
- Verify that the HA configurations match between the HA members. The `HA mode`, `group-name`, `group-id`, and `password` settings should be the same. Different `group-id` values will result in different virtual MAC addresses, which might not cause a MAC conflict. However, an IP conflict can still occur.
- If everything seems to be in working order, run `get system ha status` to verify that HA has formed successfully.

To avoid a split brain scenario:

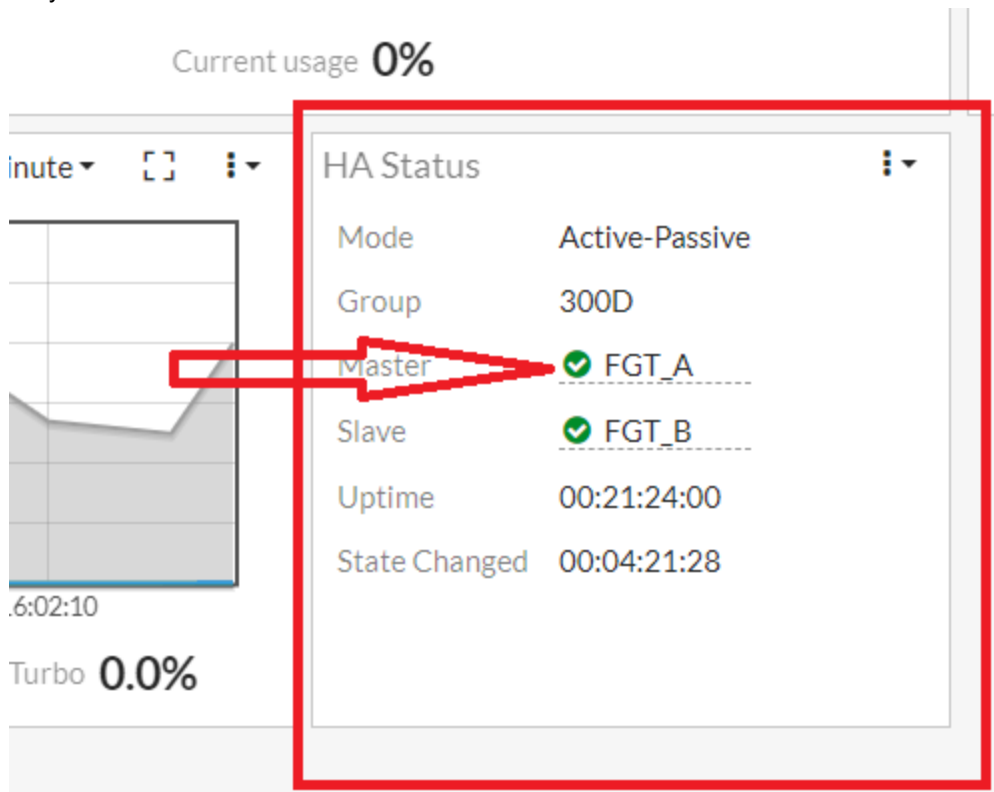
- In a two-member HA configuration, use back-to-back links for heartbeat interface instead of connecting through a switch.
- Use redundant HA heartbeat interfaces.
- In a configuration where members are in different locations, ensure the heartbeat lost intervals and thresholds are longer than the possible latency in the links.

## Check HA sync status

The HA sync status can be viewed in the GUI through either a widget on the *Dashboard* or on the *System > HA* page. It can also be confirmed through the CLI. When a cluster is out of sync, administrators should correct the issue as soon as possible as it affects the configuration integrity and can cause issues to occur.

## HA sync status in the GUI

- Dashboard widget:
  - Following HA setup, the *HA Status* widget can be added to the *Dashboard*. The widget shows the HA sync status by displaying a green checkmark next to each member in sync. A red mark indicates the member is out of sync.



- System* > *HA* page:
  - The same set of icons will be displayed on the *System* > *HA* page to indicate if the member is in sync.

|                | Synchronized          | Priority | Hostname | Role   | Uptime      | Sessions | Throughput  | AV Events | Bytes     | CPU | IPS Events | Packets | RAM |
|----------------|-----------------------|----------|----------|--------|-------------|----------|-------------|-----------|-----------|-----|------------|---------|-----|
| FortiGate 300D | NGMT1 1 2 3 4 5 6 7 8 |          |          |        |             |          |             |           |           |     |            |         |     |
| FortiGate 300D | NGMT2 1 2 3 4 5 6 7 8 |          |          |        |             |          |             |           |           |     |            |         |     |
| FortiGate 300D | NGMT1 1 2 3 4 5 6 7 8 |          | FGT_A    | Master | 00:21:22:32 | 41       | 144.00 kbps | 0         | 144.80 MB | 0%  | 0          | 486091  | 26% |
| FortiGate 300D | NGMT2 1 2 3 4 5 6 7 8 |          | FGT_B    | Slave  | 00:21:30:02 | 6        | 30.00 kbps  | 0         | 10.50 MB  | 0%  | 0          | 21526   | 25% |

## HA sync status in the CLI

- In the CLI, run the command `get sys ha status` to see if the cluster is in sync. The sync status is reported under *Configuration Status*. In the following example, both members are in sync:

```
FGT_A # get sys ha status
```

```
HA Health Status: OK Model: FortiGate-300D Mode: HA A-P Group: 146 Debug: 0 Cluster
Uptime: 0 days 21:42:53 Cluster state change time: 2019-03-09 11:40:51 Master selected
using:
```

```
<2019/03/08 18:56:12> FGT6HD3914800153 is selected as the master because it has the
least value 0 of link-failure + pingsvr-failure.
```

```
ses_pickup: enable, ses_pickup_delay=disable override: enable Configuration Status:
```

```
FGT6HD3914800069(updated 5 seconds ago): in-sync
```

```
FGT6HD3914800153(updated 4 seconds ago): in-sync
```

```
System Usage stats:
```

```
FGT6HD3914800069(updated 5 seconds ago):
```

```
sessions=17, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=25%
```

```
FGT6HD3914800153(updated 4 seconds ago):
```

```
sessions=0, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=25%
```

```
: : : Master: FGT6HD3914800069, HA operating index = 0 Slave : FGT6HD3914800153, HA
operating index = 1
```

## Disabling stateful Sctp inspection

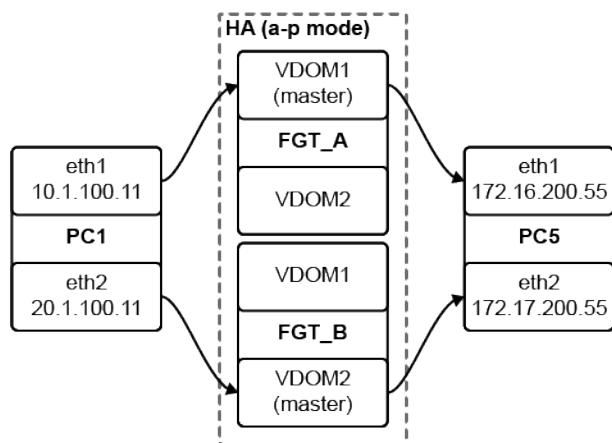
There is an option in FortiOS to disable stateful Sctp inspection. This option is useful when FortiGates are deployed in a high availability (HA) cluster that uses the FortiGate Clustering Protocol (FGCP) and virtual clustering in a multihoming topology. In this configuration, the primary stream control transmission protocol (Sctp) path traverses the primary FortiGate node by using its active VDOM (for example, VDOM1), and the backup Sctp path traverses the other passive FortiGate node by using its active VDOM (for example, VDOM2).

When stateful Sctp inspection is enabled, Sctp heartbeat traffic fails by means of the backup path because the primary path goes through a different platform and VDOM. Since there is no state sharing between VDOMs, the passive FortiGate is unaware of the original Sctp session and drops the heartbeats because of no associated sessions. When stateful Sctp inspection is disabled, the passive node permits the Sctp heartbeats to pass.

When set to `enable`, Sctp session creation without Sctp INIT is enabled. When set to `disable`, Sctp session creation without Sctp INIT is disabled (this is the default setting):

```
config system settings
 set sctp-session-without-init {enable | disable}
end
```

The following is an example topology and scenario:





In this example, FGT\_A and FGT\_B are in HA a-p mode with two virtual clusters. Two primary devices exist on different FortiGate units. PC1 eth1 can access PC5 eth1 through VDOM1, and PC1 eth2 can access PC5 eth2 through VDOM2.

On PC5, to listen for an SCTP connection:

```
sctp_darn -H 172.16.200.55 -B 172.17.200.55 -P 2500 -l
```

On PC1, to start an SCTP connection:

```
sctp_darn -H 10.1.100.11 -B 20.1.100.11 -P 2600 -c 172.16.200.55 -c 172.17.200.55 -p 2500 -s
```

An SCTP four-way handshake is on one VDOM, and a session is created on that VDOM. With the default configuration, there is no session on any other VDOM, and the heartbeat on another path (another VDOM) is dropped. After enabling `sctp-session-without-init`, the other VDOM creates the session when it receives the heartbeat, and the heartbeat is forwarded:

```
config system settings
 set sctp-session-without-init enable
end
```

## Upgrading FortiGates in an HA cluster

You can upgrade the firmware on an HA cluster in the same way as on a standalone FortiGate. During a firmware upgrade, the cluster upgrades the primary unit and all of the subordinate units to the new firmware image.



Before upgrading a cluster, back up your configuration ([Configuration backups on page 62](#)), schedule a maintenance window, and make sure that you are using a supported upgrade path (<https://docs.fortinet.com/upgrade-tool>).

## Uninterrupted upgrade

An uninterrupted upgrade occurs without interrupting communication in the cluster.

To upgrade the cluster firmware without interrupting communication, the following steps are followed. These steps are transparent to the user and the network, and might result in the cluster selecting a new primary unit.

1. The administrator uploads a new firmware image using the GUI or CLI. See [Firmware on page 626](#) for details.
2. The firmware is upgraded on all of the subordinate units.
3. A new primary unit is selected from the upgraded subordinates.
4. The firmware is upgraded on the former primary unit.
5. Primary unit selection occurs, according to the standard primary unit selection process.

If all of the subordinate units crash or otherwise stop responding during the upgrade process, the primary unit will continue to operate normally, and will not be upgraded until at least one subordinate rejoins the cluster.

## Interrupted upgrade

An interrupted upgrade upgrades all cluster members at the same time. This takes less time than an uninterrupted upgrade, but it interrupts communication in the cluster. Interrupted upgrade is disabled by default.

**To enable interrupted upgrade:**

```
config system ha
 set uninterruptible-upgrade disable
end
```

## Out-of-band management with reserved management interfaces

As part of an HA configuration, you can reserve up to four management interfaces to provide direct management access to all cluster units. For each reserved management interface, you can configure a different IP address, administrative access, and other interface settings, for each cluster unit. By connecting these interfaces to your network, you can separately manage each cluster unit from different IP addresses.

- Reserved management interfaces provide direct management access to each cluster unit, and give each cluster unit a different identity on your network. This simplifies using external services, such as SNMP, to monitor and manage separate cluster units.
- Reserved management interfaces are not assigned HA virtual MAC addresses. They retain the permanent hardware address of the physical interface, unless you manually change it using the `config system interface` command.
- Reserved management interfaces and their IP addresses should not be used for managing a cluster using FortiManager. To manage a FortiGate HA cluster with FortiManager, use the IP address of one of the cluster unit interfaces.
- Configuration changes to a reserved management interface are not synchronized to other cluster units. Other configuration changes are automatically synchronized to all cluster units.



You can configure an in-band management interface for a cluster unit. See [In-band management on page 697](#) for information. In-band management does not reserve the interface exclusively for HA management.

---

## Management interface

Enable HTTPS or HTTP administrative access on the reserved management interfaces to connect to the GUI of each cluster unit. On secondary units, the GUI has the same features as the primary unit, except for unit specific information, for example:

- The System Information widget on the Status dashboard shows the secondary units serial number.
- In the cluster members list at *System > HA*, you can change the HA configuration of the unit that you are logged into. You can only change the host name and device priority of the primary and other secondary units.
- The system events logs shows logs for the device that you are logged into. Use the HA device drop down to view the log messages for other cluster units, including the primary unit.

Enable SSH administrative access on the reserved management interfaces to connect to the CLI of each cluster unit. The CLI prompt includes the host of the cluster unit that you are connected to. Use the `execute ha manage` command to connect to other cluster unit CLIs.

Enable SNMP administrative access on a reserved management interface to use SNMP to monitor each cluster unit using the interface's IP address. Direct management of cluster members must also be enabled, see [Configuring SNMP remote management of individual cluster units example on page 693](#).

Reserved management interfaces are available in both NAT and transparent mode, and when the cluster is operating with multiple VDOMs.

## FortiCloud, FortiSandbox, and other management services

By default, management services such as FortiCloud, FortiSandbox, SNMP, remote logging, and remote authentication, use a cluster interface. This means that communication from each cluster unit will come from a cluster interface, and not from the individual cluster unit's interface.

You can configure HA reserved management interfaces to be used for communication with management services by enabling the `ha-direct` option. This separates management traffic for each cluster unit, and allows each unit to be individually managed. This is especially useful when cluster unit are in different physical locations.

The following management features will then use the HA reserved management interface:

- Remote logging, including syslog, FortiAnalyzer, and FortiCloud
- SNMP queries and traps
- Remote authentication and certificate verification
- Communication with FortiSandbox

The HA reserved management interfaces can also be configured for only SNMP remote management, see [Configuring SNMP remote management of individual cluster units example on page 693](#).

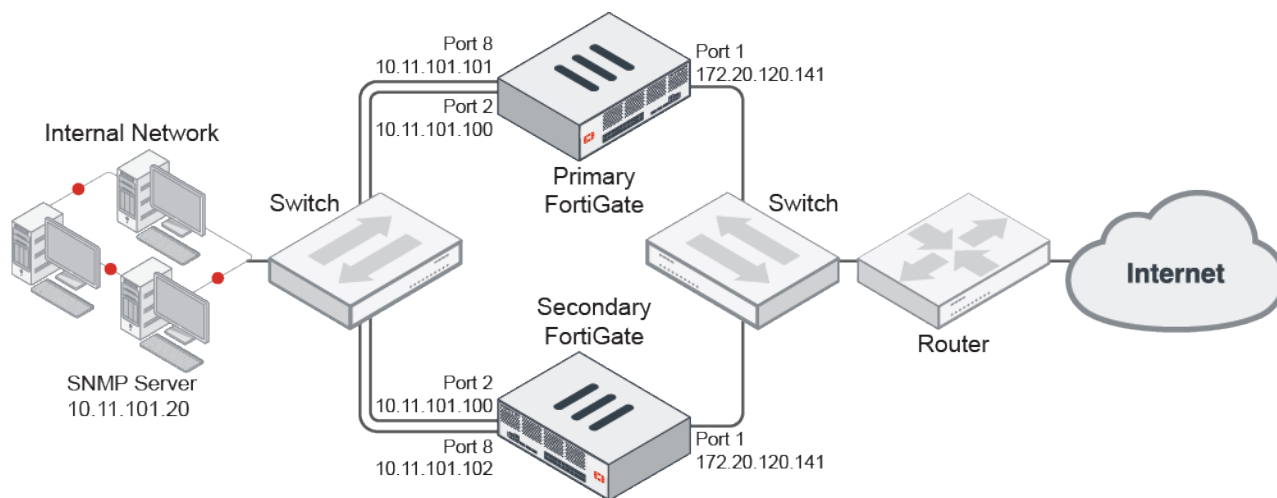
### To configure HA reserved management interfaces for communication with management services:

```
config system ha
 set ha-direct enable
end
```



Enabling `ha-direct` in a non-HA environment will make SNMP unusable.

## Configuring SNMP remote management of individual cluster units example



In this example, two FortiGate units are already operating in a cluster. On each unit, port8 is connected to the internal network through a switch and configured as a reserved management interface with SNMP remote management.



Configuration changes to the reserved management interface are not synchronized to other cluster units.

### To configure management interface reservation in the GUI:

1. Go to *System > HA* and edit the primary unit.
2. Enable *Management Interface Reservation*.
3. Set *Interface* to *port8*. This interface must not be referenced anywhere else.
4. Set *Gateway* to *10.11.101.2*. The gateway is not synchronized to secondary units.

5. Optionally, enter a *Destination subnet* to indicate the destinations that should use the defined gateway. By default, 0.0.0.0/0 is used.
6. Click **OK**.

### To configure management interface reservation in the CLI:

```
config system ha
 set ha-mgmt-status enable
 config ha-mgmt-interfaces
 edit 1
 set interface "port8"
 set gateway 10.11.101.2
 next
 end
end
```

The reserved management interface default route is not synchronized to other cluster units.

### GUI access

To configure the primary unit's reserved management interface, configure an IP address and management access on port8. Then, to configure the secondary unit's reserved management interface, access the unit's CLI through the primary unit, and configure an IP address and management access on port8. Configuration changes to the reserved management interface are not synchronized to other cluster units.

**To configure the primary unit reserved management interface to allow GUI access in the CLI:**

1. From a computer on the internal network, connect to the CLI at 10.11.101.100.
2. Change the port8 IP address and management access:

```
config system interface
 edit port8
 set ip 10.11.101.101/24
 set allowaccess https ping ssh snmp
 next
end
```

You can now log into the primary unit's GUI by browsing to <https://10.11.101.101>. You can also log into the primary unit's CLI by using an SSH client to connect to 10.11.101.101.

**To configure secondary unit reserved management interfaces to allow GUI access:**

1. From a computer on the internal network, connect to the primary unit's CLI.
2. Connect to the secondary unit with the following command:

```
execute ha manage <unit id> <username> <password>
```

3. Change the port8 IP address and management access:

```
config system interface
 edit port8
 set ip 10.11.101.102/24
 set allowaccess https ping ssh snmp
 next
end
exit
```

You can now log into the secondary unit's GUI by browsing to <https://10.11.101.102>. You can also log into the secondary unit's CLI by using an SSH client to connect to 10.11.101.102.

## SNMP management

The SNMP server can get status information from the cluster members. To use the reserved management interfaces, you must add at least one HA direct management host to an SNMP community. If the SNMP configuration includes SNMP users with user names and passwords, HA direct management must be enabled for the users.

**To configure the cluster for SNMP management using the reserved management interfaces in the CLI:**

1. Add an SNMP community with a host for the reserved management interface of each cluster member. The host includes the IP address of the SNMP server.

```
config system snmp community
 edit 1
 set name "Community"
 config hosts
 edit 1
 set ip 10.11.101.20 255.255.255.255
 set ha-direct enable
 next
 end
```

```
next
end
```



Enabling `ha-direct` in a non-HA environment will make SNMP unusable.

---

## 2. Add an SNMP user for the reserved management interface

```
config system snmp user
 edit "1"
 set notify-hosts 10.11.101.20
 set ha-direct enable
 next
end
```



The SNMP configuration is synchronized to all cluster units.

---

**To get CPU, memory, and network usage information from the SNMP manager for each cluster unit using the reserved management IP addresses:**

1. Connect to the SNMP manager CLI.
2. Get resource usage information for the primary unit using the MIB fields:

```
snmpget -v2c -c Community 10.11.101.101 fgHaStatsCpuUsage
snmpget -v2c -c Community 10.11.101.101 fgHaStatsMemUsage
snmpget -v2c -c Community 10.11.101.101 fgHaStatsNetUsage
```

3. Get resource usage information for the primary unit using the OIDs:

```
snmpget -v2c -c Community 10.11.101.101 1.3.6.1.4.1.12356.101.13.2.1.1.3.1
snmpget -v2c -c Community 10.11.101.101 1.3.6.1.4.1.12356.101.13.2.1.1.4.1
snmpget -v2c -c Community 10.11.101.101 1.3.6.1.4.1.12356.101.13.2.1.1.5.1
```

4. Get resource usage information for the secondary unit using the MIB fields:

```
snmpget -v2c -c Community 10.11.101.102 fgHaStatsCpuUsage
snmpget -v2c -c Community 10.11.101.102 fgHaStatsMemUsage
snmpget -v2c -c Community 10.11.101.102 fgHaStatsNetUsage
```

5. Get resource usage information for the primary unit using the OIDs:

```
snmpget -v2c -c Community 10.11.101.102 1.3.6.1.4.1.12356.101.13.2.1.1.3.1
snmpget -v2c -c Community 10.11.101.102 1.3.6.1.4.1.12356.101.13.2.1.1.4.1
snmpget -v2c -c Community 10.11.101.102 1.3.6.1.4.1.12356.101.13.2.1.1.5.1
```

## Firewall local-in policies for the reserved management interface

Enabling `ha-mgmt-intf-only` applies the local-in policy only to the VDOM that contains the reserved management interface. The incoming interface is set to match any interface in the VDOM..

**To add local-in policies for the reserved management interface:**

```
config firewall local-in-policy
 edit 0
 set ha-mgmt-intf-only enable
 set intf any
 set srcaddr internal-net
 set dstaddr mgmt-int
 set action accept
 set service HTTPS
 set schedule weekdays
 next
end
```

**NTP over reserved management interfaces**

If reserved management interfaces are configured for each cluster member, and NTP is enabled, then the primary unit will contact the NTP server using the reserved management interface. The system time is then synchronized to the secondary units over the HA heartbeat interface.

```
config system interface
 edit port5
 set ip 172.16.79.46 255.255.255.0
 next
end

config system ha
 set group-name FGT-HA
 set mode a-p
 set ha-mgmt-status enable
 config ha-mgmt-interfaces
 edit 1
 set interface port5
 set gateway 172.16.79.1
 next
 end
 set ha-direct enable
end

config system ntp
 set ntpsync enable
 set syncinterval 5
end
```

**In-band management**

In-band management IP addresses are an alternative to reserved HA management interfaces, and do not require reserving an interface exclusively for management access. They can be added to multiple interfaces on each cluster unit.

The in-band management IP address is accessible from the network that the cluster interface is connected to. It should be in the same subnet as the interface that you are adding it to. It cannot be in the same subnet as other interface IP addresses.

In-band management interfaces support ping, HTTP, HTTPS, and SNMP administrative access options.

Primary and secondary units send packets differently from an interface with a management IP address configured:

- On the primary unit, packets are sent to destinations based on routing information.
- On secondary units, packets can only be sent to destinations with the same management IP address segment.



In-band management IP address configuration is not synchronized to other cluster units.

---

**To add an in-band management IP address to port23 with HTTPS, SSH, and SNMP access:**

```
config system interface
 edit port23
 set management-ip 172.25.12.5/24
 set allowaccess https ssh snmp
 next
end
```

## HA cluster setup examples

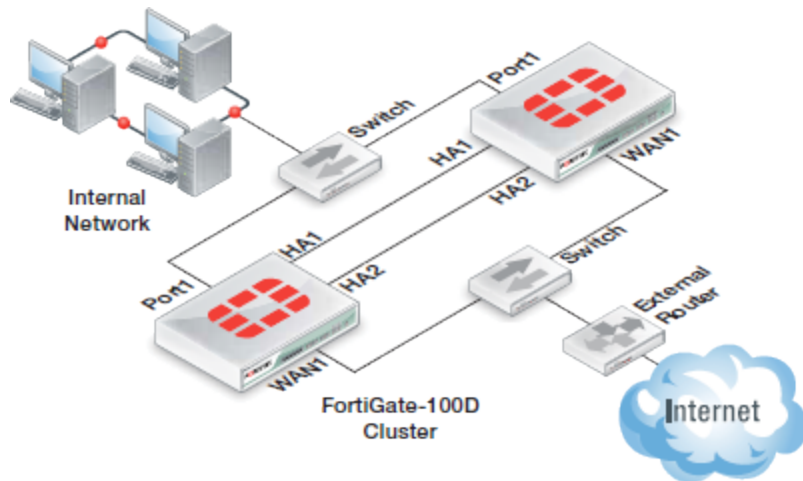
The following examples provide instructions on HA cluster setup:

- [HA active-passive cluster setup on page 698](#)
- [HA active-active cluster setup on page 700](#)
- [HA virtual cluster setup on page 701](#)
- [HA using a hardware switch to replace a physical switch on page 704](#)

### HA active-passive cluster setup

An HA Active-Passive (A-P) cluster can be set up using the GUI or CLI.

This example uses the following network topology:



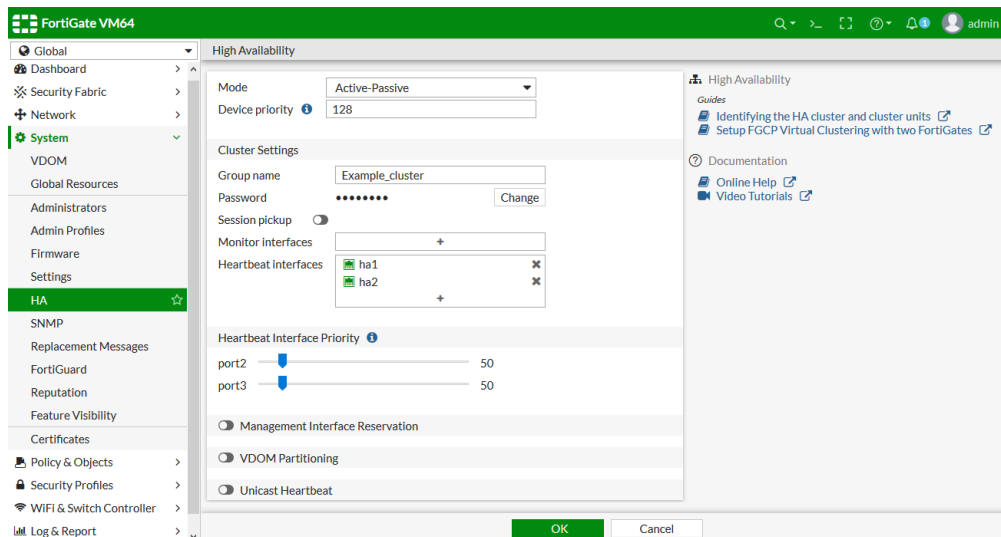


### To set up an HA A-P cluster using the GUI:

1. Make all the necessary connections as shown in the topology diagram.
2. Log into one of the FortiGates.
3. Go to *System > HA* and set the following options:

|                      |                 |
|----------------------|-----------------|
| Mode                 | Active-Passive  |
| Device priority      | 128 or higher   |
| Group name           | Example_cluster |
| Heartbeat interfaces | ha1 and ha2     |

Except for the device priority, these settings must be the same on all FortiGates in the cluster.



4. Leave the remaining settings as their default values. They can be changed after the cluster is in operation.
5. Click **OK**.  
The FortiGate negotiates to establish an HA cluster. Connectivity with the FortiGate may be temporarily lost as the HA cluster negotiates and the FGCP changes the MAC addresses of the FortiGate's interfaces.
6. Factory reset the other FortiGate that will be in the cluster, configure GUI access, then repeat steps 1 to 5, omitting setting the device priority, to join the cluster.

### To set up an HA A-P cluster using the CLI:

1. Make all the necessary connections as shown in the topology diagram.
2. Log into one of the FortiGates.
3. Change the hostname of the FortiGate:

```
config system global
 set hostname Example1_host
end
```

Changing the host name makes it easier to identify individual cluster units in the cluster operations.

4. Enable HA:

```
config system ha
 set mode a-p
```

```

set group-name Example_cluster
set hbdev ha1 10 ha2 20
end

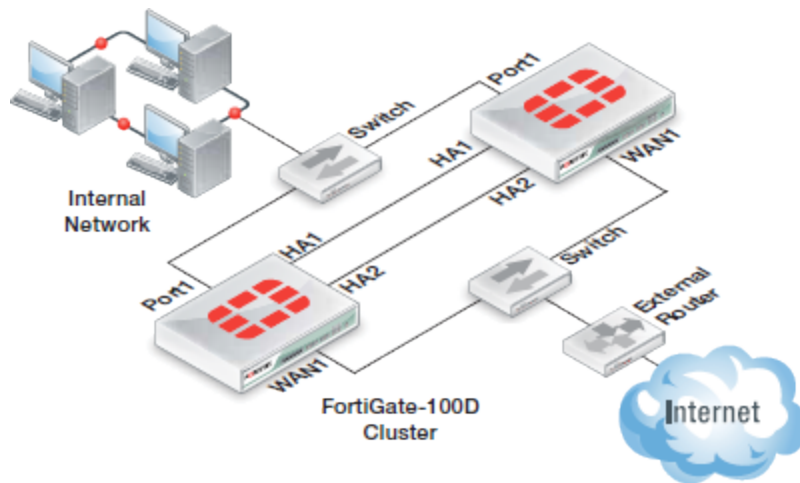
```

5. Leave the remaining settings as their default values. They can be changed after the cluster is in operation.
6. Repeat steps 1 to 5 on the other FortiGate devices to join the cluster.

## HA active-active cluster setup

An HA Active-Active (A-A) cluster can be set up using the GUI or CLI.

This example uses the following network topology:

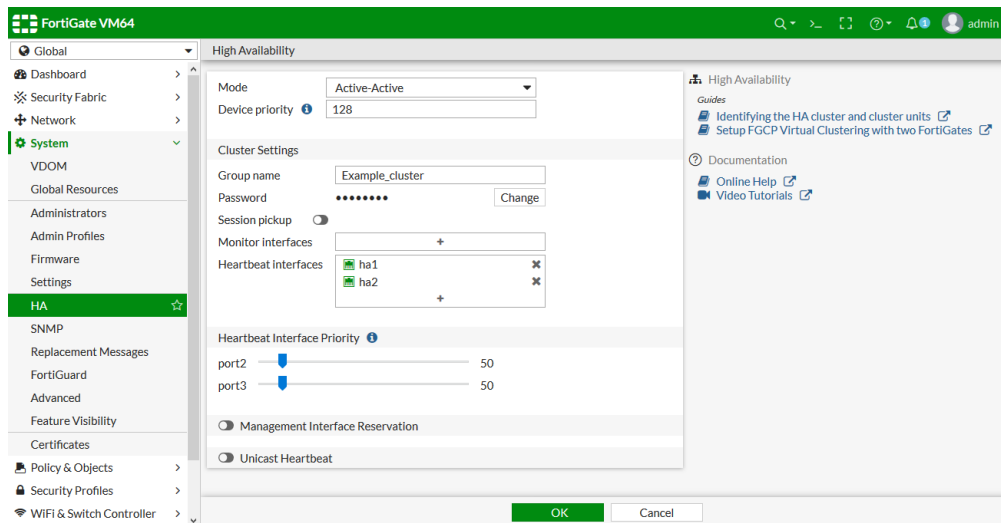


### To set up an HA A-A cluster using the GUI:

1. Make all the necessary connections as shown in the topology diagram.
2. Log into one of the FortiGates.
3. Go to *System > HA* and set the following options:

|                      |                 |
|----------------------|-----------------|
| Mode                 | Active-Active   |
| Device priority      | 128 or higher   |
| Group name           | Example_cluster |
| Heartbeat interfaces | ha1 and ha2     |

Except for the device priority, these settings must be the same on all FortiGates in the cluster.



4. Leave the remaining settings as their default values. They can be changed after the cluster is in operation.
5. Click OK.  
The FortiGate negotiates to establish an HA cluster. Connectivity with the FortiGate may be temporarily lost as the HA cluster negotiates and the FGCP changes the MAC addresses of the FortiGate's interfaces.
6. Factory reset the other FortiGate that will be in the cluster, configure GUI access, then repeat steps 1 to 5, omitting setting the device priority, to join the cluster.

### To set up an HA A-A cluster using the CLI:

1. Make all the necessary connections as shown in the topology diagram.
2. Log into one of the FortiGates.
3. Change the hostname of the FortiGate:

```
config system global
 set hostname Example1_host
end
```

Changing the host name makes it easier to identify individual cluster units in the cluster operations.

4. Enable HA:

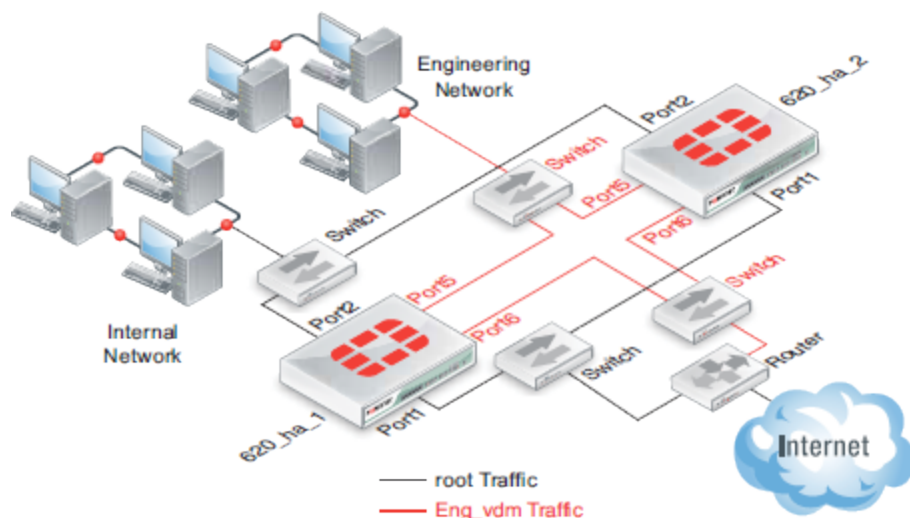
```
config system ha
 set mode a-a
 set group-name Example_cluster
 set hbdev ha1 10 ha2 20
end
```

5. Leave the remaining settings as their default values. They can be changed after the cluster is in operation.
6. Repeat steps 1 to 5 on the other FortiGate devices to join the cluster.

## HA virtual cluster setup

An HA virtual cluster can be set up using the GUI or CLI.

This example uses the following network topology:



HA virtual clusters are based on VDOMs and are more complicated than regular clusters.



The root VDOM can only be associated with virtual cluster 1.  
The VDOM that is assigned as the management VDOM can also only be associated with virtual cluster 1.

### To set up an HA virtual cluster using the GUI:

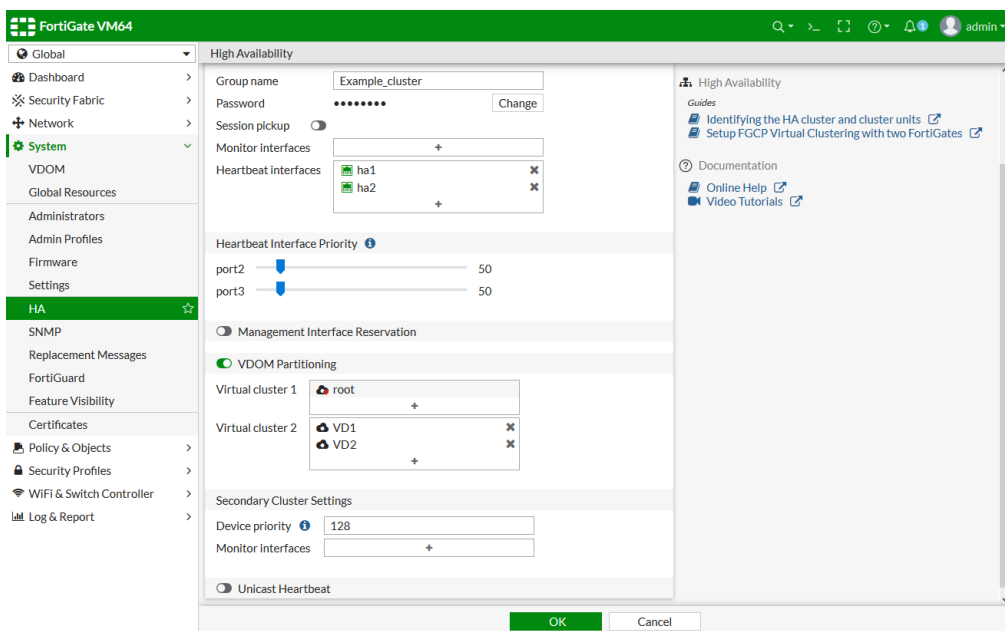
1. Make all the necessary connections as shown in the topology diagram.
2. Log into one of the FortiGates.
3. Go to *System > HA* and set the following options:

|                      |                 |
|----------------------|-----------------|
| Mode                 | Active-Passive  |
| Device priority      | 128 or higher   |
| Group name           | Example_cluster |
| Heartbeat interfaces | ha1 and ha2     |

Except for the device priority, these settings must be the same on all FortiGates in the cluster.

4. Leave the remaining settings as their default values. They can be changed after the cluster is in operation.
5. Click *OK*.  
The FortiGate negotiates to establish an HA cluster. Connectivity with the FortiGate may be temporarily lost as the HA cluster negotiates and the FGCP changes the MAC addresses of the FortiGate's interfaces.
6. Factory reset the other FortiGate that will be in the cluster, configure GUI access, then repeat steps 1 to 5, omitting setting the device priority, to join the cluster.
7. Go to *System > Settings* and enable *Virtual Domains*.
8. Click *Apply*. You will be logged out of the FortiGate.
9. Log back into the FortiGate, ensure that you are in the global VDOM, and go to *System > VDOM*.

10. Create two new VDOMs, such as VD1 and VD2:
  - a. Click *Create New*. The *New Virtual Domain* page opens.
  - b. Enter a name for the VDOM in the *Virtual Domain* field, then click *OK* to create the VDOM.
  - c. Repeat these steps to create a second new VDOM.
11. Implement a virtual cluster by moving the new VDOMs to *Virtual cluster 2*:
  - a. Go to *System > HA*.
  - b. Enable *VDOM Partitioning*.
  - c. Click on the *Virtual cluster 2* field and select the new VDOMs.



- d. Click *OK*.

### To set up an HA virtual cluster using the CLI:

1. Make all the necessary connections as shown in the topology diagram.
2. Set up a regular A-P cluster. See [HA active-passive cluster setup on page 698](#).
3. Enable VDOMs:

```
config system global
 set vdom-mode multi-vdom
end
```

You will be logged out of the FortiGate.

4. Create two VDOMs:

```
config vdom
 edit VD1
 next
 edit VD2
 next
end
```

### 5. Reconfigure the HA settings to be a virtual cluster:

```
config global
 config system ha
 set vcluster2 enable
 config secondary-vcluster
 set vdom "VD1" "VD2"
 end
 end
end
```

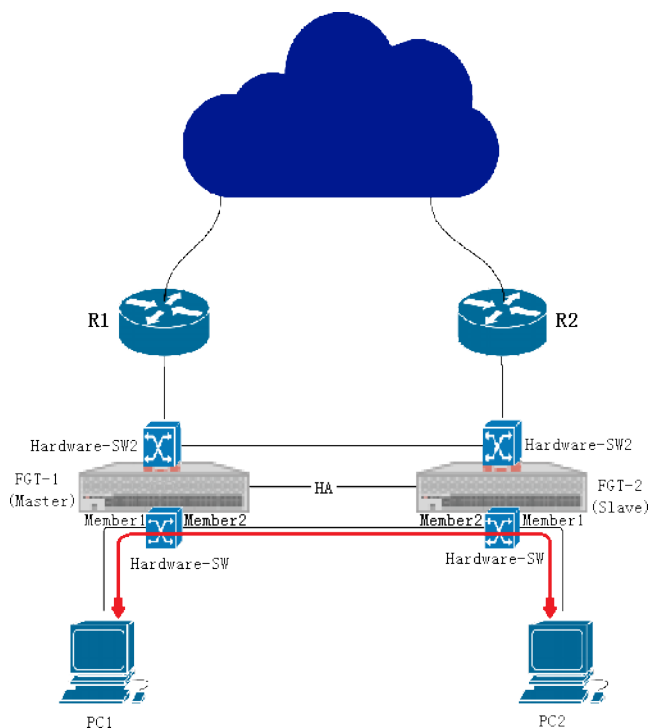
## HA using a hardware switch to replace a physical switch

Using a hardware switch to replace a physical switch is not recommended, as it offers no redundancy or interface monitoring.

- If one FortiGate loses power, all of the clients connected to that FortiGate device cannot go to another device until that FortiGate recovers.
- A hardware switch cannot be used as a monitor interface in HA. Any incoming or outgoing link failures on hardware member interfaces will not trigger failover; this can affect traffic.

## Examples

The examples use the following topology:



## Traffic between hardware switches

When using Hardware switch in HA environment, a client device connected to the hardware switch on the primary FortiGate can communicate with client devices connected to the hardware switch on secondary FortiGates as long as

there is a direct connection between the two switches.

No configuration is required after setting up the hardware switches. If a client connected to both of the hardware switches needs to reach destinations outside of the cluster, the firewall must be configured for it.

### To configure the FortiGate devices:

1. Connect the devices as shown in the topology diagram.
2. On each FortiGate, configure HA:

```
config system ha
 set mode a-a
 set group-name Example_cluster
 set hbdev ha1 10 ha2 20
end
```

3. On the primary FortiGate, configure the hardware switch:

```
config system virtual-switch
 edit Hardware-SW
 set physical-switch sw0
 config port
 edit port3
 next
 edit port5
 next
 end
 next
end
```

4. On each FortiGate, configure the IP addresses on the hardware switches:

```
config system interface
 edit Hardware-SW
 set ip 6.6.6.1 255.255.255.0
 set allowaccess ping ssh http https
 next
end
```

After configuring the hardware switches, PC1 and PC2 can now communicate with each other.

### Traffic passes through FortiGate

If client device needs to send traffic through the FortiGate, additional firewall configuration on the FortiGate is required.

All traffic from the hardware switches on either the primary or secondary FortiGate reaches the primary FortiGate first. The traffic is then directed according to the HA mode and firewall configuration.

### To configure the FortiGate devices:

1. Connect the devices as shown in the topology diagram.
2. On each FortiGate, configure HA:

```
config system ha
 set mode a-a
 set group-name Example_cluster
```

```
 set hbdev hal 10 ha2 20
 end
```

**3. On the primary FortiGate, configure the hardware switch:**

```
config system virtual-switch
 edit Hardware-SW
 set physical-switch sw0
 config port
 edit port3
 next
 edit port5
 next
 end
 next
 edit Hardware-SW2
 set physical-switch sw0
 config port
 edit port1
 next
 end
 next
end
```

**4. On each FortiGate, configure the IP addresses on the hardware switch:**

```
config system interface
 edit Hardware-SW
 set ip 6.6.6.1 255.255.255.0
 set allowaccess ping ssh http https
 next
 edit Hardware-SW2
 set ip 172.16.200.1 255.255.255.0
 set allowaccess ping ssh http https
 next
end
```

**5. On each FortiGate, configure a firewall policy:**

```
config firewall policy
 edit 1
 set srcintf Hardware-SW
 set dstintf Hardware-SW2
 set srcaddr all
 set dstaddr all
 set service ALL
 set action accept
 set schedule always
 set nat enable
 next
end
```

**6. On each FortiGate, configure a static route:**

```
config router static
 edit 1
 set device Hardware-SW2
 set gateway 172.16.200.254
```



```
 next
end
```

Traffic from PC1 and PC2 can now reach destinations outside of the FortiGate cluster.

## SNMP

SNMP enables you to monitor hardware on your network. You can configure the hardware, such as the FortiGate SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers. SNMP traps alert you to events that happen, such as when a log disk is full or a virus is detected.

The FortiGate SNMP implementation is read-only. SNMP v1/v2c, and v3 compliant SNMP managers have read-only access to FortiGate system information through queries, and can receive trap messages from the FortiGate unit.

- [Interface access on page 707](#)
- [MIB files on page 708](#)
- [SNMP agent on page 708](#)
- [SNMP v1/v2c communities on page 709](#)
- [SNMP v3 users on page 710](#)
- [Important SNMP traps on page 712](#)

### Interface access

Before a remote SNMP manager can connect to the FortiGate SNMP agent, you must configure one or more FortiGate interfaces to accept SNMP connections.

#### To configure a FortiGate interface to accept SNMP connections in the GUI:

1. Go to *Network > Interfaces*.
2. Edit the interface.
3. In the *Administrative Access* options, enable *SNMP*.
4. Click *OK*.

#### To configure a FortiGate interface to accept SNMP connections in the CLI:

```
config system interface
 edit <interface>
 append allowaccess snmp
 set snmp-index <integer>
 config ipv6
 append ip6-allowaccess snmp
 end
 next
end
```

## MIB files

The FortiGate SNMP agent supports Fortinet proprietary MIBs, as well as the parts of RFC 2665 and RFC 1213 that apply to FortiGate unit configuration.

Your SNMP manager may already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet proprietary MIBs to this database to have access to Fortinet specific information.

| MIB file or RFC              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FORTINET-CORE-MIB.mib        | The Fortinet core MIB includes all system configuration and trap information that is common to all Fortinet products.<br>Your SNMP manager requires this information to monitor Fortinet device settings and receive traps from the FortiGate SNMP agent.                                                                                                                                                                                          |
| FORTINET-FORTIGATE-MIB.mib   | The FortiGate MIB includes all system configuration information and trap information that is specific to FortiGate units.<br>Your SNMP manager requires this information to monitor FortiGate settings and receive traps from the FortiGate SNMP agent.                                                                                                                                                                                            |
| RFC-1213 (MIB II)            | The FortiGate SNMP agent supports MIB II groups with the following exceptions: <ul style="list-style-type: none"><li>• No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10).</li><li>• Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not accurately capture all Fortinet traffic activity. More accurate information can be obtained from the information reported by the Fortinet MIB.</li></ul> |
| RFC-2665 (Ethernet-like MIB) | The FortiGate SNMP agent supports Ethernet-like MIB information.<br>FortiGate SNMP does not support for the dot3Tests and dot3Errors groups.                                                                                                                                                                                                                                                                                                       |

### To download the MIB files:

1. Go to *System > SNMP*.
2. Click *Download FortiGate MIB File* and save the file to the management computer.
3. Click *Download Fortinet Core MIB File* and save the file to the management computer.

## SNMP agent

The SNMP agent sends SNMP traps originating on the FortiGate to an external monitoring SNMP manager defined in a SNMP community. The SNMP manager can monitor the FortiGate system to determine if it is operating properly, or if any critical events occurring.

The description, location, and contact information for this FortiGate system will be part of the information that the SNMP manager receives. This information is useful if the SNMP manager is monitoring many devices, and enables faster responses when the FortiGate system requires attention.

### To configure the SNMP agent in the GUI:

1. Go to *System > SNMP*.
2. Enable *SNMP Agent*.
3. Enter a description of the agent.

4. Enter the location of the FortiGate unit.
5. Enter a contact or administrator for the SNMP Agent or FortiGate unit.
6. Click *Apply*.

**To configure the SNMP agent in the CLI:**

```
config system snmp sysinfo
 set status enable
 set description <string>
 set contact-info <string>
 set location <string>
end
```

## SNMP v1/v2c communities

An SNMP community is a grouping of equipment for network administration purposes. A single device can belong to multiple communities.

You must add an SNMP community to the FortiGate so that the SNMP manager can receive traps and system information. Up to three communities can be added.

**To create a n SNMP v1/v2c community in the GUI:**

1. Go to *System > SNMP*.
2. In the *SNMP v1/v2c* table, click *Create New*.

FortiGate 60E

DocsFG-60E

Dashboard
Security Fabric
FortiView
Network
System
Administrators
Admin Profiles
Firmware
Settings
HA
SNMP
Replacement Messages
Replacement Message Groups
FortiGuard
Reputation
Advanced
Feature Visibility
Certificates
Policy & Objects
Security Profiles
VPN
User & Device
WiFi & Switch Controller
Log & Report
Monitor

SNMP

Download FortiView

System Information

SNMP Agent

Description

Location

Contact Info

SNMP v1/v2c

Create New

Name

doeco

SNMP v3

Create New

Name

Sec

New SNMP Community

Community Name

Enabled

Hosts

IP Address

Host Type

Accept queries and send traps

IP Address

Host Type

Queries

v1 Enabled

Port

161

v2c Enabled

Port

161

Traps

v1 Enabled

Local Port

162

Remote Port

162

v2c Enabled

Local Port

162

Remote Port

162

SNMP Events

CPU usage too high

Available memory low

OK

Cancel

3. Enter a *Community Name* and enable the community.
4. In the *Hosts* section, enter the *IP Address* and select the *Host Type* for each SNMP manager.
5. In the *Queries* section, enable or disable v1 and v2c queries, then enter the port numbers that the SNMP managers in this community use for them.
6. In the *Traps* section, enable or disable v1 and v2c traps, then enter the local and remote port numbers that the SNMP managers in this community use for them.

7. In the *SNMP Events* section, enable or disable the events that activate traps in this community.
8. Click **OK**.

**To create a n SNMP v1/v2c community in the CLI:**

```
config system snmp community
 edit 2
 set name <string>
 set status {enable | disable}
 config hosts
 edit <host_id>
 set ip <ip/mask>
 set source-ip <class_ip>
 set ha-direct {enable | disable}
 set host-type {any | query | trap}
 next
 end
 set query-v1-port <port_number>
 set query-v1-status {enable | disable}
 set query-v2c-port <port_number>
 set query-v2c-status {enable | disable}
 set trap-v1-lport <port_number>
 set trap-v1-rport <port_number>
 set trap-v1-status {enable | disable}
 set trap-v2c-lport <port_number>
 set trap-v2c-rport <port_number>
 set trap-v2c-status {enable | disable}
 set events <events>
 next
end
```

## SNMP v3 users

Authentication is used to ensure the identity of users. Privacy allows for encryption of SNMP v3 messages to ensure confidentiality of data. These protocols provide a higher level of security than is available in SNMP v1 and v2c, which use community strings for security. Both authentication and privacy are optional.

### To create a n SNMP v3 user in the GUI:

1. Go to *System > SNMP*.
2. In the *SNMP v3* table, click *Create New*.

3. Enter a *Use Name* and enable the user.
4. In the *Security Level* section, configure the security level:
  - *No Authentication*: No authentication or encryption.
  - *Authentication*: Select the authentication algorithm and password.
  - *Authentication and Private*: Select both the authentication and encryption algorithms and password.
5. In the *Hosts* section, enter the *IP Address* for each SNMP manager.
6. In the *Queries* section, enable or disable queries, then enter the port number that the SNMP managers use for them.
7. In the *Traps* section, enable or disable traps, then enter the local and remote port numbers that the SNMP managers use for them.
8. In the *SNMP Events* section, enable or disable the events that activate traps.
9. Click *OK*.

### To create an SNMP v3 user in the CLI:

```
config system snmp user
 edit <user>
 set status {enable | disable}
 set trap-status {enable | disable}
 set trap-lport <port_number>
 set trap-rport <port_number>
 set queries {enable | disable}
 set query-port <port_number>
 set notify-hosts <class_ip> ... <class_ip>
 set source-ip <class_ip>
 set ha-direct {enable | disable}
 set events <events>
 set security-level {no-auth-no-priv | auth-no-priv | auth-priv}
```

```

 set auth-proto {md5 | sha}
 set auth-pwd <password>
 set prive-proto {aes | des | aes256 | aes256cisco}
 set priv-pwd <password>
next
end

```

## Important SNMP traps

### Link Down and Link Up traps

This trap is sent when a FortiGate port either goes down or is brought up.

For example, the following traps are generated when the state of port34 is set to down using `set status down`, and then brought up using `set status up`:

```

NET-SNMP version 5.7.3 2019-01-31 14:11:48 10.1.100.1(via UDP: [10.1.100.1]:162->
[10.1.100.11]:162) TRAP, SNMP v1, community REGR-SYS SNMPv2-MIB::snmpTraps Link Down Trap
(0) Uptime: 0:14:44.95 IF-MIB::ifIndex.42 = INTEGER: 42 IF-MIB::ifAdminStatus.42 = INTEGER:
down(2) IF-MIB::ifOperStatus.42 = INTEGER: down(2) FORTINET-CORE-MIB::fnSysSerial.0 =
STRING: FG140P3G15800330 SNMPv2-MIB::sysName.0 = STRING: FortiGate-140D-POE

2019-01-31 14:11:48 <UNKNOWN> [UDP: [10.1.100.1]:162->[10.1.100.11]:162]: DISMAN-EVENT-
MIB::sysUpTimeInstance = Timeticks: (88495) 0:14:44.95 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-
MIB::linkDown IF-MIB::ifIndex.42 = INTEGER: 42 IF-MIB::ifAdminStatus.42 = INTEGER: down(2)
IF-MIB::ifOperStatus.42 = INTEGER: down(2) FORTINET-CORE-MIB::fnSysSerial.0 = STRING:
FG140P3G15800330 SNMPv2-MIB::sysName.0 = STRING: FortiGate-140D-POE 2019-01-31 14:12:01
10.1.100.1(via UDP: [10.1.100.1]:162->[10.1.100.11]:162) TRAP, SNMP v1, community REGR-SYS
SNMPv2-MIB::snmpTraps Link Up Trap (0) Uptime: 0:14:57.98 IF-MIB::ifIndex.42 = INTEGER: 42
IF-MIB::ifAdminStatus.42 = INTEGER: up(1) IF-MIB::ifOperStatus.42 = INTEGER: up(1) FORTINET-
CORE-MIB::fnSysSerial.0 = STRING: FG140P3G15800330 SNMPv2-MIB::sysName.0 = STRING:
FortiGate-140D-POE

2019-01-31 14:12:01 <UNKNOWN> [UDP: [10.1.100.1]:162->[10.1.100.11]:162]: DISMAN-EVENT-
MIB::sysUpTimeInstance = Timeticks: (89798) 0:14:57.98 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-
MIB::linkUp IF-MIB::ifIndex.42 = INTEGER: 42 IF-MIB::ifAdminStatus.42 = INTEGER: up(1) IF-
MIB::ifOperStatus.42 = INTEGER: up(1) FORTINET-CORE-MIB::fnSysSerial.0 = STRING:
FG140P3G15800330 SNMPv2-MIB::sysName.0 = STRING: FortiGate-140D-POE

```

### fgFmTrapIfChange trap

This trap is sent when any changes are detected on the interface. The change can be very simple, such as giving an IPV4 address.

For example, the user has given the IP address of 1.2.3.4/24 to port 1 and the EMS Manager has detected the following trap:

```

DISMAN-EXPRESSION-MIB::sysUpTimeInstance = Timeticks: (7975058) 22:09:10.58 SNMPv2-
MIB::snmpTrapOID.0 = OID: FORTINET-FORTIGATE-MIB::fgFmTrapIfChange FORTINET-CORE-
MIB::fnSysSerial.0 = STRING: FG140P3G15800330 IF-MIB::ifName.45 = STRING: port1 FORTINET-
FORTIGATE-MIB::fgManIfIp.0 = IpAddress: 1.2.3.4 FORTINET-FORTIGATE-MIB::fgManIfMask.0 =
IpAddress: 255.255.255.0 FORTINET-FORTIGATE-MIB::fgManIfIp6.0 = STRING: 0:0:0:0:0:0:0:0

```

## entConfigChange trap

The change to the interface in the previous example has also triggered the *ConfChange Trap* which is sent along with the *fgFmTrapIfChange* trap:

```
2018-11-15 09:30:23 FGT_A [UDP: [172.16.200.1]:162->[172.16.200.55]:162]: DISMAN-EXPRESSION-MIB::sysUpTimeInstance = Timeticks: (8035097) 22:19:10.97 SNMPv2-MIB::snmpTrapOID.0 = OID: ENTITY-MIB::entConfigChange
```

## fgTrapDeviceNew trap

This trap is triggered when a new device, like a FortiSwitch, is connected to the FortiGate.

For example, the following scenario has given the device a new trap for adding FortiAP on a PoE interface a FortiGate 140D-POE. The trap has important information about the device name, device MAC address, and when it was last seen.

```
2018-11-15 11:17:43 UDP/IPv6: [2000:172:16:200::1]:162 [UDP/IPv6: [2000:172:16:200::1]:162]: DISMAN-EXPRESSION-MIB::sysUpTimeInstance = Timeticks: (520817) 1:26:48.17 SNMPv2-MIB::snmpTrapOID.0 = OID: FORTINET-FORTIGATE-MIB::fgTrapDeviceNew FORTINET-CORE-MIB::fnSysSerial.0 = STRING: FG140P3G15800330 SNMPv2-MIB::sysName.0 = STRING: FGT_A IF-MIB::ifIndex.0 = INTEGER: 0 FORTINET-FORTIGATE-MIB::fgVdEntIndex.0 = INTEGER: 0 FORTINET-FORTIGATE-MIB::fgDeviceCreated.0 = Gauge32: 5 FORTINET-FORTIGATE-MIB::fgDeviceLastSeen.0 = Gauge32: 5 FORTINET-FORTIGATE-MIB::fgDeviceMacAddress.0 = STRING: 90:6c:ac:f9:97:a0
```

```
2018-11-15 11:17:43 FGT_A [UDP: [172.16.200.1]:162->[172.16.200.55]:162]: DISMAN-EXPRESSION-MIB::sysUpTimeInstance = Timeticks: (520817) 1:26:48.17 SNMPv2-MIB::snmpTrapOID.0 = OID: FORTINET-FORTIGATE-MIB::fgTrapDeviceNew FORTINET-CORE-MIB::fnSysSerial.0 = STRING: FG140P3G15800330 SNMPv2-MIB::sysName.0 = STRING: FGT_A IF-MIB::ifIndex.0 = INTEGER: 0 FORTINET-FORTIGATE-MIB::fgVdEntIndex.0 = INTEGER: 0 FORTINET-FORTIGATE-MIB::fgDeviceCreated.0 = Gauge32: 5 FORTINET-FORTIGATE-MIB::fgDeviceLastSeen.0 = Gauge32: 5 FORTINET-FORTIGATE-MIB::fgDeviceMacAddress.0 = STRING: 90:6c:ac:f9:97:a0
```

## fgTrapAvOversize trap

The *fgTrapAvOversize* trap is generated when the antivirus scanner detects an oversized file:

```
019-01-31 13:22:04 10.1.100.1(via UDP: [10.1.100.1]:162->[10.1.100.11]:162) TRAP, SNMP v1, community REGR-SYS FORTINET-FORTIGATE-MIB::fgt140P Enterprise Specific Trap (602) Uptime: 1 day, 3:41:10.31 FORTINET-CORE-MIB::fnSysSerial.0 = STRING: FG140P3G15800330 SNMPv2-MIB::sysName.0 = STRING: FortiGate-140D-POE 2019-01-31 13:22:29 <UNKNOWN> [UDP: [10.1.100.1]:162->[10.1.100.11]:162]: DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (9967031) 1 day, 3:41:10.31 SNMPv2-MIB::snmpTrapOID.0 = OID: FORTINET-FORTIGATE-MIB::fgTrapAvOversize FORTINET-CORE-MIB::fnSysSerial.0 = STRING: FG140P3G15800330 SNMPv2-MIB::sysName.0 = STRING: FortiGate-140D-POE
```

## Replacement messages

The replacement message list in *System > Replacement Messages* enables you to view and customize replacement messages. Highlight the replacement messages you want to edit and customize the message content to your requirements. Hit **Save** when done. If you do not see the message you want to edit, select the *Extended View* option in the upper right-hand corner of the screen.

If you make a mistake, select *Restore Default* to return to the original message and code base.

## Replacement message images

You can add images to replacement messages on:

- Disclaimer pages
- Login pages
- Declined disclaimer pages
- Login failed pages
- Login challenge pages
- Keepalive pages

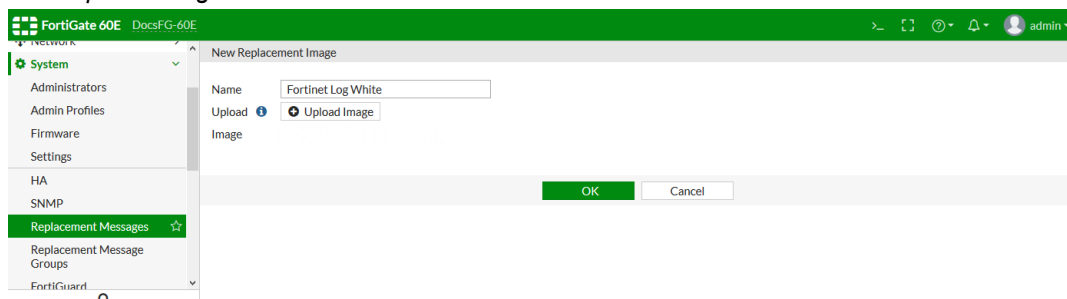


Supported image formats are GIF, JPEG, TIFF, and PNG. The maximum file size supported is 24KB.

## Adding images to replacement messages

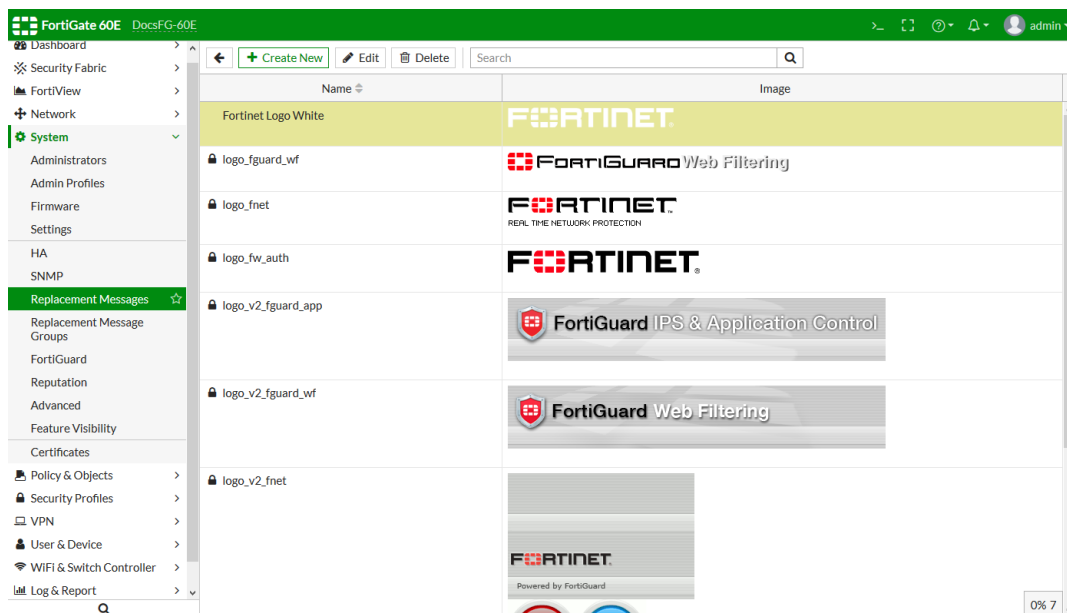
To add images to replacement messages in the GUI:

1. Go to *System > Replacement Messages*.
2. Click *Manage Images* at the top of the page.
3. Click *Create New*.
4. Enter a name for the image.
5. Click *Upload Image* and locate the file.





## 6. Click OK.



## To add images to replacement messages in the CLI:

```
config system replacemsg-image
 edit <image_name>
 set image-type {gif | jpg | tiff | png}
 set image-base64 <string>
 next
end
```

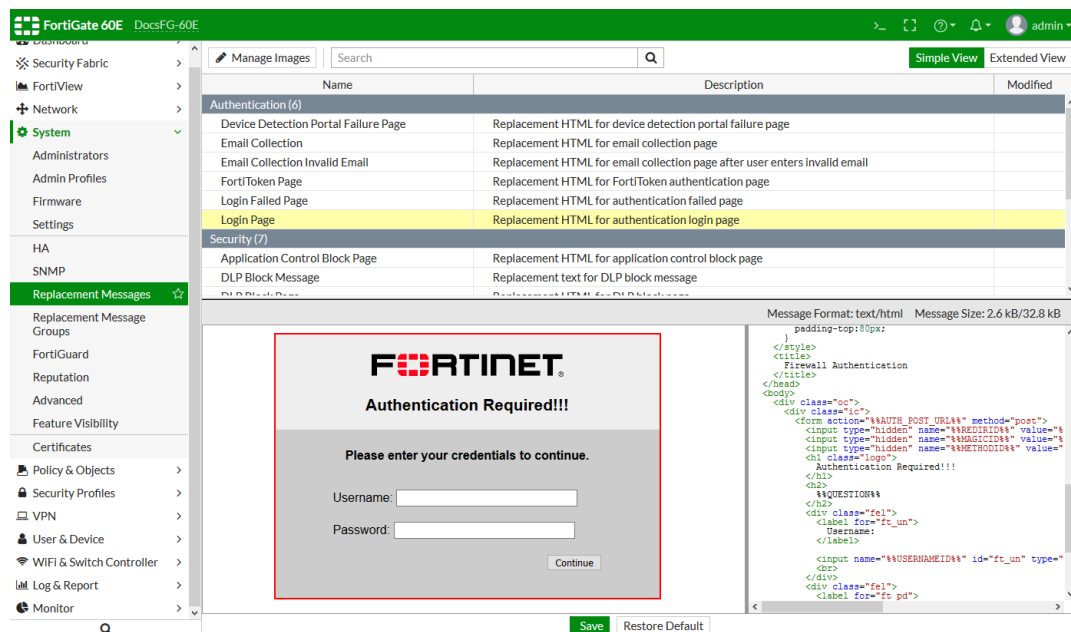
## Modifying replacement messages

Replacement messages can be modified to include an HTML message or content that suits your organization. A list of common replacement messages appear in the main window. Select *Extended View* to see the entire list and all categories for replacement messages.

## To modify a replacement message in the GUI:

1. Go to *System > Replacement Messages*.
2. Select the replacement message you want to edit.
3. In the bottom pane of the GUI the message will be displayed on the left alongside the HTML code on the right. Edit the HTML code as needed.

The message view changes in real-time as you edit the content.



4. Click Save.

### To modify a replacement message in the CLI:

```
config system replacemsg <message_category> <message_type>
 set buffer <string>
 set header {none | http | 8bit}
 set format {none | text | html}
end
```

For example, to modify the *Traffic Quota Limit Exceeded Page* message:

```
config system replacemsg traffic-quota "per-ip-shaper-block"
 set buffer "<html>
<head>
 <title>
 Traffic Quota Control
 </title>
</head>
<body>

 <table width=\"100%\">
 <tr>
 <td bgcolor=#3300cc align=\"center\" colspan=2>

 Traffic blocked because exceeded session quota

 </td>
 </tr>
 </table>

 Traffic blocked because it exceeded the per IP shaper session quota. Please contact
```

```
the system administrator.

 %%QUOTA_INFO%%

 <hr>

</body>
</html>"
 set header http
 set format html
end
```

## Replacement message groups

Replacement message groups allow you to customize replacement messages for individual policies and profiles.

There are two types of replacement message groups:

- **utm:** Used with UTM settings in firewall policies. Messages in the following categories can be customized: mail, http, webproxy, ftp, nntp, fortiguard-wf, spam, alertmail, admin, sslvpn, nac-quar, traffic-quota, utm, custom-message, and icap.
- **auth:** Used with authentication pages in firewall policies. Messages in the following categories can be customized: webproxy and auth.

The messages added to a group do not need to be customized. The body content, header type, and format of a message will use the default values if not customized.

### To create or edit a replacement message group in the CLI:

```
config system replacemsg-group
 edit <group>
 set group-type {auth | utm}
 config <message_category>
 edit <message_type>
 set buffer <message>
 set header {none | http | 8bit}
 set format {none | text | html}
 next
 end
 next
end
```

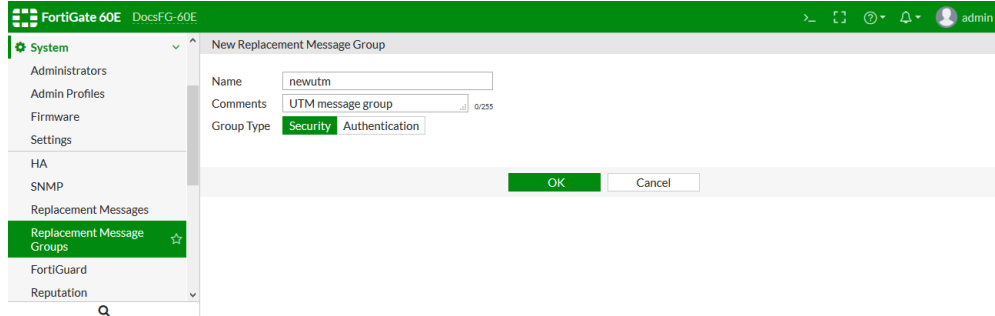
### To create a replacement message group in the GUI:

1. Make replacement message groups visible in the GUI with the following CLI command:

```
config system settings
 set gui-replacement-message-groups enable
end
```

2. Go to *System > Replacement Message Groups*.
3. Click *Create New*.

4. Enter a name for the new group.
5. Optionally, enter a comment describing the group.
6. Select the *Group Type*, either *Security* or *Authentication*.



7. Click OK.

## Example

In this example, two replacement message groups are created. The UTM type message group includes custom mail related messages, changes the formats of some spam related message, and is assigned to an email filter profile. The authentication type message group has a custom authentication success message that is applied to a proxy-based firewall policy that with the email filter profile assigned.

**To create the replacement message groups and use them in a profile and a policy in the CLI:**

1. Create the replacement message groups:

```
config system replacemsg-group
 edit "newutm"
 set group-type utm
 config mail
 edit "partial"
 set buffer "Fragmented emails are blocked, sorry."
 next
 edit "email-av-fail"
 set buffer "The email has been blocked for reasons."
 next
 end
 config spam
 edit "submit"
 set header http
 set format html
 next
 edit "reversedns"
 set header http
 set format html
 next
 end
 next
 edit "newauth"
 set group-type auth
 config auth
 edit "auth-success-msg"
```

```
 set buffer "Welcome to the firewall. Your authentication has been
accepted, please reconnect."
 set header none
 set format text
 next
end
next
end
```

## 2. Apply the message groups:

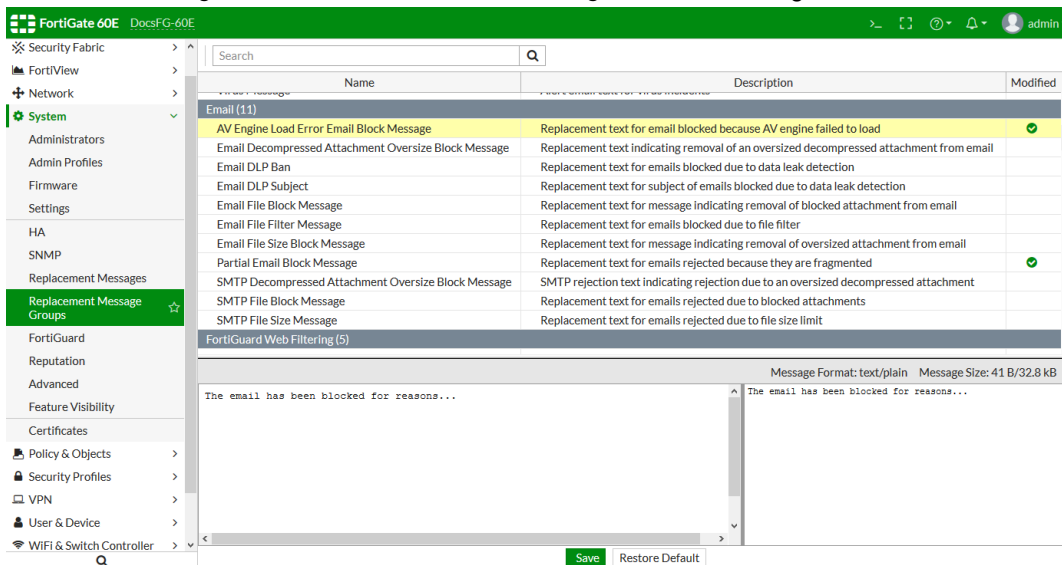
```
config emailfilter profile
 edit "newmsgs"
 set replacemsg-group "newutm"
 next
end

config firewall policy
 edit 1
 ...
 set replacemsg-override-group "newauth"
 set inspection-mode proxy
 set emailfilter-profile "newmsgs"
 ...
 next
end
```

## To create the replacement message groups and use them in a profile and a policy in the GUI:

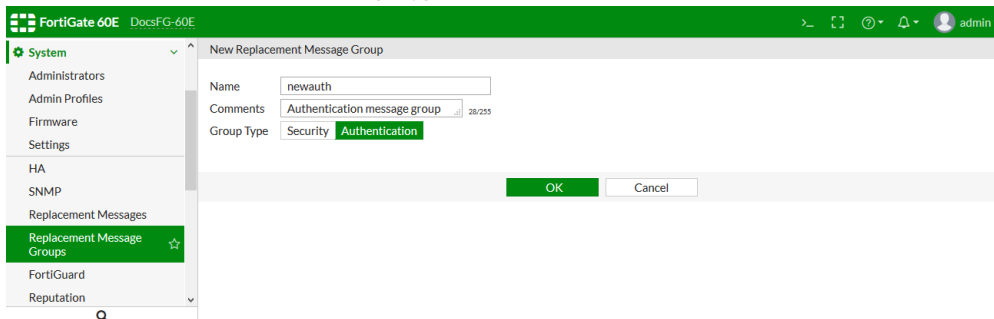
1. Create the *Security* replacement message groups:
  - a. Go to *System > Replacement Message Groups*.
  - b. Click *Create New*.
  - c. Enter *newutm* in the *Name* field.
  - d. Enter *UTM message group* in the *Comments* field.
  - e. Select *Security* as the *Group Type*.
  - f. Click *OK*.
2. Customize the replacement messages in the *newutm* group:
  - a. Go to *System > Replacement Message Groups*.
  - b. Edit the *newutm* group.

- c. Locate the *AV Engine Load Error Email Block Message*, edit the message, then click **Save**.



- d. Locate the *Partial Email Block Message*, edit the message, then click **Save**.

3. Create the *Authentication* replacement message group:
- Go to *System Replacement Message Groups*.
  - Click **Create New**.
  - Enter *newauth* in the *Name* field.
  - Enter *Authentication message group* in the *Comments* field.
  - Select *Authentication* as the *Group Type*.



- f. Click **OK**.

- Apply the *newutm* replacement message group to an email filter profile using the CLI.
- Apply the *newauth* replacement message group and the email filter profile to a firewall policy using the CLI.

## FortiGuard

FortiGuard services can be purchased and registered to your FortiGate unit. The FortiGate must be connected to the Internet in order to automatically connect to the FortiGuard Distribution Network (FDN) to validate the license and download FDN updates.

The FortiGuard subscription update services include:

- Antivirus (AV)
- Intrusion Protection Service (IPS)
- Application Control
- Antispam
- Web Filtering
- Web Application Firewall (WAF)

To view FDN support contract information, go to *System > FortiGuard*. The *License Information* table shows the status of your FortiGate's support contract.

- [IPv6 FortiGuard connections on page 721](#)
- [Configuring antivirus and IPS options on page 722](#)
- [Manual updates on page 722](#)
- [Automatic updates on page 723](#)
- [Sending malware statistics to FortiGuard on page 725](#)
- [Update server location on page 725](#)
- [Filtering on page 726](#)
- [Override FortiGuard servers on page 727](#)
- [Online security tools on page 727](#)
- [FortiGuard third party SSL validation and anycast support on page 728](#)

## IPv6 FortiGuard connections

The Fortinet DNS can resolve FortiGuard related servers to both IPv4 and IPv6 addresses. FortiOS daemons (update, forticld, url) connect using either IPv4 or IPv6 addresses. The first available connection will be used for updates or the rating service.

### To configure an interface and route for IPv6:

```
config system interface
 edit "wan1"
 set vdom "root"
 config ipv6
 set ip6-address 2000:172:16:200::1/64
 end
 next
end

config router static6
 edit 1
 set gateway 2000:172:16:200::254
 set device "wan1"
 next
end
```

### To configure push updates:

```
config system autoupdate push-update
 set status enable
 set override enable
```

```
set address "2620:101:9005:3860::94"
end
```

## Configuring antivirus and IPS options

### To configure antivirus and IPS options:

1. Go to *System > FortiGuard*
2. Scroll down to the *AntiVirus & IPS Updates* section.
3. Configure the antivirus and IPS options for connecting and downloading definition files:

<b>Accept push updates</b>	Enable to allow updates to be sent automatically to your FortiGate. New definitions will be added as soon as they are released by FortiGuard. See <a href="#">Push updates on page 724</a> .
<b>Use override push</b>	Only available if <i>Accept push updates</i> is enabled. See <a href="#">Override push on page 724</a> .
<b>Scheduled Updates</b>	Enable to schedule updates to be sent to the FortiGate at the specified time. See <a href="#">Scheduled updates on page 723</a> .
<b>Improve IPS quality</b>	Enable to send information to the FortiGuard servers when an attack occurs. This can help keep the FortiGuard database current as attacks evolve, and improve IPS signatures.
<b>Use extended IPS signature package</b>	Enable to use the extended IPS database, that includes protection from legacy attacks, along with the regular IPS database that protects against the latest common and in-the-wild attacks.
<b>Update AV &amp; IPS Definitions</b>	Click to manually initiate an FDN update.

4. Click *Apply*.

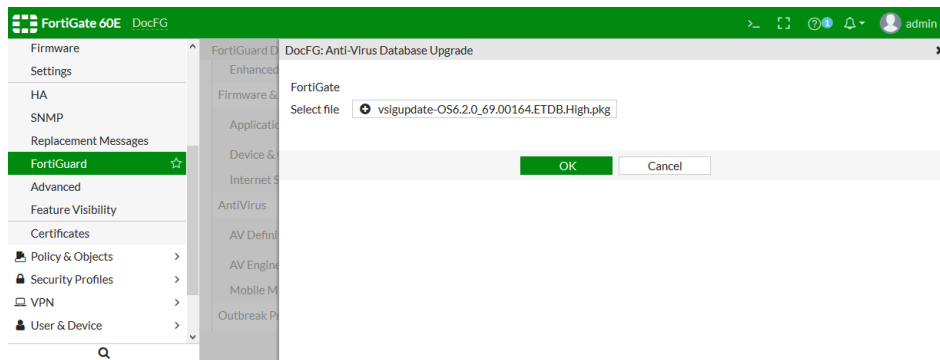
## Manual updates

When needed, FDN updates can be manually uploaded.

### To manually update the signature definitions files:

1. Log in to the [Fortinet Support](#) website.
2. Go to *Download > FortiGuard Service Updates*.
3. Select your *OS Version* from the dropdown list.
4. Locate your device in the table, and download the signature definitions files.
5. On the FortiGate, go to *System FortiGuard*.
6. In the *License Information* table, locate the row of the definitions that you are updating, and click *Upgrade Database* in the rightmost column.
7. In the pane that opens, click *Upload*, locate the downloaded definitions file on your computer, then click *Open*. The download may take a few minutes to complete.





8. Click **OK**.

## Automatic updates

The FortiGate can be configured to request updates from FDN on a schedule, or via push notification.

### Scheduled updates

Scheduling updates ensures that the virus and IPS definitions are downloaded to your FortiGate on a regular basis.

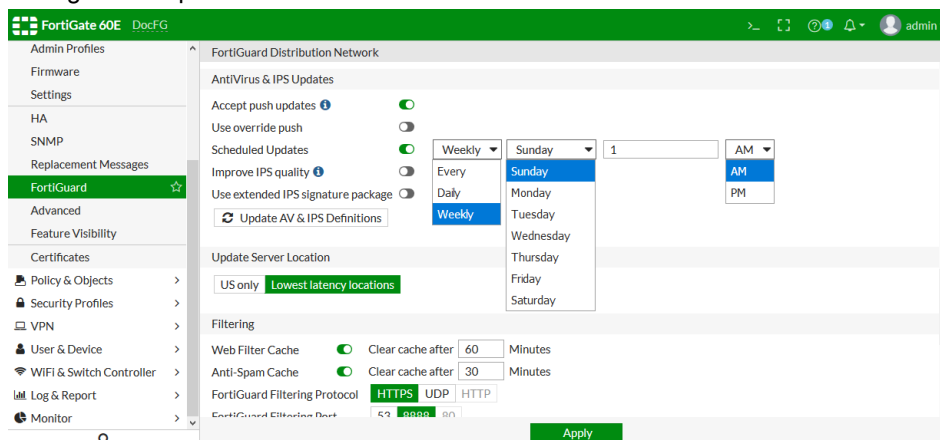
Updating definitions can cause a brief disruption in traffic that is currently being scanned while the FortiGate unit applies the new signature database. Updates should be scheduled during off-peak hours when network usage is at a minimum to ensure that network activity will not be affected by downloading the definitions files.



A schedule of once a week means any urgent updates will not be pushed until the scheduled time. If an urgent update is required, click the *Update AV & IPS Definitions* button to manually update the definitions.

### To configure scheduled updates in the GUI:

1. Go to *System > FortiGuard*
2. Scroll down to the *AntiVirus & IPS Updates* section.
3. Enable *Scheduled Updates*.
4. Configure the update schedule.



5. Click *Apply*.

### To configure scheduled updates in the CLI:

```
config system autoupdate schedule
 set status enable
 set frequency {every | daily | weekly}
 set time <hh:mm>
 set day <day_of_week>
end
```

### Push updates

Push updates enable you to get immediate updates when new viruses or intrusions are discovered and new signatures are created. This ensures that the latest signature are sent to the FortiGate as soon as possible.

When a push notification occurs, the FortiGuard server sends a notice to the FortiGate that a new signature definition file available. The FortiGate then initiates a download of the definition file. For maximum security, both scheduled and push updates should be enabled.

### To enable push updates - GUI:

1. Go to *System > FortiGuard*
2. Scroll down to the *AntiVirus & IPS Updates* section.
3. Enable *Accept push updates*.
4. Click *Apply*.

### To enable push updates in the CLI:

```
config system autoupdate push-update
 set status enable
 set override {enable | disable}
 set address <vip_address>
end
```

### Override push

If the FortiGate is behind a NAT device (or another FortiGate), or if your organization provides updates using their own FortiGuard server, an override server must be used to ensure that the FortiGate receives push update notifications. The FDS will connect to the NAT device when attempting to reach the FortiGate, and the NAT device must be configured to forward FDS traffic to the FortiGate on UDP port 9443.

Push updates must be enabled to configure a push update override.

For example, if the NAT device is another FortiGate:

1. On the FortiGate NAT device, add a port forwarding virtual IP address in *Policy & Objects > Virtual IPs*. See for details.
2. On the FortiGate NAT device, add a security policy that connects to the internet and includes the port forwarding VIP.
3. On the internal FortiGate device, configure *Push update override*.

### To configure push update override in the GUI:

1. Go to *System > FortiGuard*
2. Scroll down to the *AntiVirus & IPS Updates* section.
3. Enable *Accept push updates*.
4. Enable *Use override push*.
5. Enter the IP address and port number configured on the NAT device.
6. Click *Apply*.

### To configure push update override in the CLI:

```
config system autoupdate push-update
 set status enable
 set override {enable | disable}
 set address <vip_address>
end
```

## Sending malware statistics to FortiGuard

FortiGate devices periodically send encrypted antivirus, IPS, botnet IP list, and application control statistics to FortiGuard. Included with these data is the IP address and serial number of the FortiGate, and the country that it is in. This information is never shared with external parties, [Fortinet Privacy Policy](#).

The malware statistics are used to improve various aspects of FortiGate malware protection. For example, antivirus data allow FortiGuard to determine what viruses are currently active. Signatures for those viruses are kept in the Active AV Signature Database that is used by multiple Fortinet products. Inactive virus signatures are moved to the Extended AV Signature Database (see [Configuring antivirus and IPS options on page 722](#)). When events for inactive viruses start appearing in the malware data, the signatures are moved back into the AV Signature Database.

The FortiGate and FortiGuard servers go through a 2-way SSL/TLS 1.2 authentication before any data is transmitted. The certificates used in this process must be trusted by each other and signed by the Fortinet CA server.

The FortiGate only accepts data from authorized FortiGuard servers. Fortinet products use DNS to find FortiGuard servers and periodically update their FortiGate server list. All other servers are provided by a list that is updated through the encrypted channel.

Malware statistics are accumulated and sent every 60 minutes by default.

To configure sharing this information, use the following CLI command:

```
config system global
 set fds-statistics {enable | disable}
 set fds-statistics-period <minutes>
end
```

## Update server location

The location of the FortiGuard update server that the FortiGate connects to can be set to either only servers in the USA only, or to the servers with the lowest latency.

On hardware FortiGate devices, the default is *Lowest latency locations*. On VM devices, the default is *US only*.

### To configure the update server location in the GUI:

1. Go to *System > FortiGuard*
2. Scroll down to the *Update Server Location* section.
3. Select *US only* or *Lowest latency locations*.
4. Click *Apply*.

### To configure the update server location in the CLI:

```
config system fortiguard
 set update-server-location {usa | any}
end
```

## Filtering

Web filtering is used to block access to harmful, inappropriate, and dangerous web sites (see [FortiGuard filter on page 954](#)).

Email filtering is used to detect and block spam messages (see [FortiGuard-based filters on page 1048](#)).

### To configure filtering in the GUI:

1. Go to *System > FortiGuard*
2. Scroll down to the *Filtering* section.
3. Configure the settings as needed:

<b>Web Filter Cache</b>	Enable/disable web filter cache, and set the amount of time that the FortiGate will store a blocked IP address or URL locally. After the time expires, the FortiGate contacts the FDN to verify the address.
<b>Anti-Spam Cache</b>	Enable/disable email filter cache, and set the amount of time that the FortiGate will store an email address locally.
<b>FortiGuard Filtering Protocol</b>	Select the protocol for contacting the FortiGuard servers.
<b>FortiGuard Filtering Port</b>	Select the port assignments for contacting the FortiGuard servers.
<b>Filtering Service Availability</b>	The status of the filtering service. Click <i>Check Again</i> if the filtering service is not available.
<b>Request re-evaluation of a URL's category</b>	Click to re-evaluate a URL category rating on the FortiGuard web filter service.

4. Click *Apply*.

### To configure filtering in the CLI:

```
config system fortiguard
 set protocol {https | udp | http}
 set port {443 | 53 | 8888 | 80}
 set antispam-force-off {enable | disable}
 set antispam-cache {enable | disable}
 set antispam-cache-ttl <integer>
```

```

set antisipam-cache-mpercent <percent>
set antisipam-timeout <integer>
set webfilter-force-off {enable | disable}
set webfilter-cache {enable | disable}
set webfilter-cache-ttl <integer>
set webfilter-timeout <integer>

```

end



FortiGuard server support for HTTPS on port 443 is supported as of FortiOS 6.2.2.

## Override FortiGuard servers

By default, FortiOS will update signature packages and query rating servers using public FortiGuard servers. This list can be overridden by adding servers to the override server list. Communication with public FortiGuard servers can also be disabled.

### To add an override FortiGuard server in the GUI:

1. Go to *System > FortiGuard*
2. Scroll down to the *Override FortiGuard Servers* section.
3. In the table, click *Create New*. The *Create New Override FortiGuard Server* pane opens.
4. Select the server address type: *IPv4*, *IPv6*, or *FQDN*.
5. Enter the server address of the selected type in the *Address* field.
6. Select the type of server: *AntiVirus & IPS Updates*, *Filtering*, or *Both*.
7. Click *Apply*.

### To add an override FortiGuard server in the CLI:

```

config system central-management
 set type fortiguard
 config server-list
 edit <integer>
 set server-type {update rating}
 set server-address <ip_address>
 next
 end
end

```

## Online security tools

FortiGuard Labs provides a number of online security tools, including but not limited to:

- **URL lookup**

Enter a website address to see if it has been rated and what category and classification it is filed as. If you find a site that has been wrongly categorized, use this page to request that the site be re-evaluated:

<https://www.fortiguard.com/webfilter>

- **Threat Encyclopedia**

Browse FortiGuard Labs extensive encyclopedia of threats. Search for viruses, botnet C&C, IPS, endpoint vulnerabilities, and mobile malware: <https://www.fortiguards.com/encyclopedia>

- **Application Control**

Browse FortiGuard Labs extensive encyclopedia of applications: <https://www.fortiguards.com/appcontrol>

## FortiGuard third party SSL validation and anycast support

You can enable anycast to optimize the routing performance to FortiGuard servers. Relying on Fortinet DNS servers, the FortiGate will get a single IP address for the domain name of each FortiGuard service. BGP routing optimization is transparent to the FortiGate. The domain name of each FortiGuard service is the common name in that service's certificate. The certificate is signed by a third party intermediate CA. The FortiGuard server uses the Online Certificate Status Protocol (OCSP) stapling technique, so that the FortiGate can always validate the FortiGuard server certificate efficiently.

### To enable anycast in the FortiGuard settings:

```
config system fortiguards
 set protocol https
 set port 443
 set fortiguards-anycast enable
 set fortiguards-anycast-source fortinet
end
```

After anycast is enabled, the FortiGuard settings will enforce a connection using HTTPS and port 443.



HTTPS/443 is only supported on anycast servers. When `fortiguards-anycast` is disabled, use HTTPS/8888 or HTTPS/53.

## Connecting to the FortiGuard

The FortiGate will only complete the TLS handshake with a FortiGuard that provides a *good* OCSP status for its certificate. Any other status will result in a failed SSL connection. OCSP stapling is reflected on the signature interval (currently, 24 hours) so that *good* means that the certificate is not revoked at that timestamp. The FortiGuard servers query the CA's OCSP responder every four hours and update its OCSP status. If the FortiGuard is unable to reach the OCSP responder, it will keep the last known OCSP status for seven days. This cached OCSP status will be sent out immediately when a client connection request is made, thus optimizing the response time.

### The following steps are taken to connect to FortiGuard:

1. The FortiGate embeds the CA\_bundle certificate, which includes the root CA with CRL list and third party intermediate CA, in the root CA level.
2. The FortiGate finds the FortiGuard IP address from its domain name from DNS:  
`fds=qaupdate.fortinet.net-192.168.100.242`
3. The FortiGate starts a TLS handshake with the FortiGuard IP address. The client hello includes an extension of the *status request*.
4. The FortiGuard servers provide a certificate with its OCSP status: *good*, *revoked*, or *unknown*.

5. The FortiGate verifies the CA chain against the root CA in the CA\_bundle.
6. The FortiGate verifies the intermediate CA's revoke status against the root CA's CRL.
7. The FortiGate verifies the FortiGuard certificate's OCSP status:

OCSP Response Data:

```
OCSP Response Status: successful (0x0)
Response Type: Basic OCSP Response
Version: 1 (0x0)
Responder Id: 3DD350A5D6A0ADEEF34A600A65D321D4F8F8D60F
Produced At: Aug 20 07:50:58 2019 GMT
Responses:
Certificate ID:
 Hash Algorithm: sha1
 Issuer Name Hash: 49F4BD8A18BF760698C5DE402D683B716AE4E686
 Issuer Key Hash: 3DD350A5D6A0ADEEF34A600A65D321D4F8F8D60F
 Serial Number: 02555C9F3901B799DF1873402FA9392D
Cert Status: good
This Update: Aug 20 07:50:58 2019 GMT
Next Update: Aug 27 07:05:58 2019 GMT
```

## Using FortiManager as local FortiGuard server

FortiManager can provide a local FortiGuard server with port 443 access.

Anycast FortiGuard settings force the rating process to use port 443, even with an override server. Using a unique address in the same subnet as the FortiManager access IP address, the FortiManager can provide local FortiGuard updates and rating access with a dedicated IP address and port 443.

### To use a FortiManager as a local FortiGuard server:

```
config system central-management
 set type fortimanager
 set fmg "172.18.37.148"
 config server-list
 edit 1
 set server-type update
 set server-address 172.18.37.150
 next
 edit 2
 set server-type rating
 set server-address 172.18.37.149
 next
 end
 set fmg-update-port 443
 set include-default-servers enable
end
```

When `fmg-update-port` is set to 443, the update process will use port 443 to connect to the override update server, which is the local FortiGuard server in the FortiManager. If this is not set, the update process will use port 8890, and the server address setting has to be the FortiManager access IP address. Override FortiGuard services come from the server list that is the local FortiGuard server in the FortiManager, and use the traditional, non-OCSP TLS handshake. If override servers in the FortiManager are not available, the default FortiGuard servers are connected, and the anycast OCSP TLS handshake is used.

## Configuration scripts

Configuration scripts are text files that contain CLI command sequences. They can be created using a text editor or copied from a CLI console, either manually or using the *Record CLI Script* function.

Scripts can be used to run the same task on multiple devices. For example, if your devices use the same security policies, you can enter or record the commands to create those policies in a script, and then run the script on each device. You could also create the policies in the GUI, and then copy and paste the CLI commands from the *CLI Console* using the *show* command.

If the FortiGate is managed by FortiManager, scripts can be uploaded to FortiManager and then run on any other FortiGates that are managed by that FortiManager. See [Scripts](#) in the [FortiManager Administration Guide](#).



A comment line in a script starts with the number sign (#). Comments are not executed.

### To run a script using the GUI:

1. Click on your username and select *Configuration > Scripts*.
2. Click *Run Script*.
3. Select the text file containing the script on your management computer, then click *OK*.  
The script runs immediately, and the *Script Execution History* table is updated, showing if the script ran successfully.

Name	Result	Time
Local		
GetSystemStatus.txt	Success	2020/01/08 09:08:56
test.txt	Success	2019/09/17 08:34:30

## Workspace mode

Workspace mode allows administrators to make a batch of changes that are not implemented until the transaction is committed. Prior to committing, the changes can be reverted or edited as needed without impacting current operations.

When an object is edited in workspace mode it is locked, preventing other administrators from editing that object. A warning message will be shown to let the administrator know that the object is currently being configured in another transaction.

All administrators can use workspace mode; their permissions in workspace mode are the same as defined in their account profile.



A workspace mode transaction times out after five minutes if there is no activity. When a transaction times out, all changes are discarded. A warning message will be shown to let the administrator know that a timeout is imminent, or has already happened:

```
config transaction id=1 will expire in 30 seconds
config transaction id=1 will expire in 20 seconds
config transaction id=1 will expire in 10 seconds
config transaction id=1 has expired
```

The following commands are not changeable in a workspace transaction:

```
config system console
config system resource-limits
config system elbc
config system global
 set split-port
 set vdom-admin
 set management-vdom
 set wireless-mode
 set internal-switch-mode
end
config system settings
 set opmode
end
config system npu
config system np6
config system wireless
 set mode
end
config system vdom-property
config system storage
```

The `execute batch` command cannot be used in or to start workspace mode.

### To use workspace mode:

#### 1. Start workspace mode:

```
execute config-transaction
```

Once in workspace mode, the administrator can make configuration changes, all of which are made in a local CLI process that is not viewable by other processes.

#### 2. Commit configuration changes:

```
execute config-transaction commit
```

After performing the commit, the changes are available for all other processes, and are also made in the kernel.

#### 3. Abort configuration changes:

```
execute config-transaction abort
```

If changes are aborted, no changes are made to the current configuration or the kernel.

### Diagnose commands

```
diagnose sys config-transaction show txn-meta
```

Show config transaction meta information. For example:

```
diagnose sys config-transaction show txn-meta
txn_next_id=8, txn_nr=2
```

```
diagnose sys config-transaction show txn-info
```

Show config transaction information. For example:

```
diagnose sys config-transaction show txn-info
current_jiffies=680372
```

```
txn_id=6, expire_jiffies=706104, clicmd_fpath='/dev/cmdb/txn/6_EiLl9G.conf'
txn_id=7, expire_jiffies=707427, clicmd_fpath='/dev/cmdb/txn/7_UXK6wY.conf'
```

```
diagnose sys config-transaction show txn-entity
```

Show config transaction entity. For example:

```
diagnose sys config-transaction show txn-entity
vd='global', cli-node-oid=37(system.vdom), txn_id=7. location: fileid=0, storeid=0,
pgnr=0, pgidx=0
vd='global', cli-node-oid=46(system.interface), txn_id=7. location: fileid=3,
storeid=0, pgnr=0, pgidx=0
```

```
diagnose sys config-transaction show txn-lock
```

Show transaction lock status. For example:

```
diagnose sys config-transaction show txn-lock
type=-1, refcnt=0, value=256, pid=128
```

```
diagnose sys config-transaction status
```

Show the transaction status in the current CLI.

## Feature visibility

Feature visibility is used to control which features are visible in the GUI. This allows features that are not in use to be hidden. Some features are also invisible by default and must be made visible before they can be configured in the GUI.

The visibility of a feature does not affect its functionality or configuration. Invisible features can still be configured using the CLI.

### To change the visibility of features:

1. Go to *System > Feature Visibility*.
2. Change the visibility of the features as required. To simplify setting security features, a feature set can be selected from the dropdown list.  
For information about what settings each option affects, click on the + icon to the right of the feature name.  
Changes are listed on the right of the screen.
3. Click *Apply*.

## Security feature presets

Six system presets are available:

- *NGFW*: for networks that require application control and protection from external attacks.
- *ATP*: for networks that require protection from viruses and other external threats.
- *WF*: for networks that require web filtering.

- *NGFW + ATP*: for networks that require protection from external threats and attacks.
- *UTM*: for networks that require protection from external threats and wish to use security features that control network usage. This is the default setting.
- *Full UTM*: for networks that require the normal UTM features, as well as antivirus, application control, endpoint control, and web filtering.
- *Custom* should be chosen for networks that require customization of available features (including the ability to select all features).

## Certificates

FortiOS leverages certificates in multiple areas, such as VPNs, administrative access, and deep packet inspection. This section contains topics about uploading certificates and provides examples of how certificates may be used to encrypt and decrypt communications, and represent the identity of the FortiGate. This section assumes the reader has a high level understanding of the public key infrastructure (PKI) system, particularly how entities leverage trusted certificate authorities (CAs) to verify the authenticating party, and how public and private certificate keys work to secure communications.

The certificates feature is hidden by default in FortiOS. In the GUI, go to *System > Feature Visibility* and enable *Certificates*.

The following topics provide an overview of how to add certificates to the FortiGate:

- [Uploading a certificate using the GUI on page 733](#)
- [Uploading a certificate using the CLI on page 736](#)
- [Uploading a certificate using an API on page 737](#)

The following topics provide examples of how to use certificates:

- [Microsoft CA deep packet inspection on page 745](#)
- [Procure and import a signed SSL certificate on page 741](#)
- [Provision a trusted certificate with Let's Encrypt on page 750](#)
- [Creating certificates with XCA on page 753](#)

## Uploading a certificate using the GUI

On the *System > Certificates* page, there are two options to add a certificate: *Generate* (use a certificate signing request) and *Import*.

### Generate certificate signing request

Certificate signing requests (CSRs) are used to generate a certificate which is then signed by a CA to create a chain of trust. The CSR includes details of the FortiGate (see table below) and its public key. A CSR is not strictly necessary; some CAs allow you to provide the details of the FortiGate manually, but a CSR helps streamline the process. Selecting *Generate* takes you the *Generate Certificate Signing Request* page to enter the following information:

<b>Certificate Name</b>	Enter the certificate name; this is how it will appear in the <i>Local Certificates</i> list.
-------------------------	-----------------------------------------------------------------------------------------------

<b>Subject Information</b>	Specify an ID type: IP, domain name (FQDN), or email address.
<b>Optional Information</b>	<p>Although listed as optional, we recommended entering the information for each field in this section.</p> <p>If you are generating a CSR for a third-party CA, you need to insure that these values reflect those listed for your company or organization at said certificate authority. If you are generating a certificate for a Microsoft CA, you need to check with the administrator regarding these values.</p>
<b>Organization Unit</b>	Enter the name of the organizational unit under which the certificate will be issued.
<b>Organization</b>	Enter the overall name of the organization.
<b>Locality(City)</b>	Enter the city where the SSL certificate is located.
<b>State / Province</b>	Some issuers will reject a CSR that has an abbreviated state or province, so enter the full name of the state or province.
<b>Country / Region</b>	Enable the option and select the country from the dropdown.
<b>E-Mail</b>	Enter the email address of the technical contact for the SSL certificate that is being requested.
<b>Subject Alternative Name</b>	This field allows multiple domains to be used in an SSL certificate. Select from email addresses, IP addresses, URIs, DNS names, and so on.
<b>Password for private key</b>	If supplied, this is used as an encryption password for the private key file.
<b>Key Type</b>	RSA is the base selection for this field and the only supported algorithm.
<b>Key Size</b>	Select either 1024, 1536, 2048, or 5096 for bit-size/strength. We recommend using at least 2048 if your CA can issue certificates of that size.
<b>Curve Name</b>	When <i>Key Type</i> is <i>Elliptic Curve</i> , select the elliptic curve type: secp256r1, secp384r1, or secp521r1.
<b>Enrollment Method</b>	<p>Select one of the following methods that determines how the CSR will be signed.</p> <ul style="list-style-type: none"> <li>• <i>File Based</i>: this will generate a certificate in the certificate menu under <i>Local Certificate</i>, which differs from the existing ones because it has no <i>Subject</i>, <i>Comments</i>, <i>Issuer</i>, or <i>Expires</i> values in the table. It will also show a <i>Pending</i> status because it is only a CSR at the moment and cannot function as a certificate just yet. You can download the CSR to provide to a CA for signing. If you open the CSR file, it should look similar to this:</li> </ul> <pre>-----BEGIN CERTIFICATE REQUEST----- MIIC7jCCAdYCAQAwwZUxCzAJBgNVBAYT (... )HEKjDX+Hg== -----END CERTIFICATE REQUEST-----</pre> <p>Next, the CSR file is supplied to a CA for signing and the returned file from the CA should be in .CER format. This file is then uploaded to the FortiGate by going to <i>System &gt; Certificates &gt; Import &gt; Local Certificate</i> and uploading the CER file.</p>

- **Online SCEP:** the Simple Certificate Enrollment Protocol (SCEP) allows devices to enroll for a certificate by using a URL and a password. The SCEP server works as a proxy to forward the FortiGate's request to the CA and returns the result to the FortiGate (setting up an SCEP server is beyond the scope of this topic). Once the request is approved by the SCEP server, the FortiGate will have a signed certificate containing the details provided in the CSR.

## Import

Although *Import* is often used in conjunction with a CSR, you may upload a certificate to the FortiGate that was generated on its own. This is typical of wildcard certificates (\*.domain.tld) where the same certificate is used across multiple devices (FGT.domain.tld, FAZ.domain.tld, and so on), but may be used for individual certificates so long as the information provided to the signing CA matches that of the FortiGate.

When selecting *Import*, there are four options: *Local Certificate*, *CA Certificate*, *Remote Certificate*, and *CRL*.

### Local certificate

Local certificates are used by the FortiGate to identify itself, or a service it provides, such as HTTPS administrative access, SSL VPN user portal, or virtual server load balancing where the FortiGate masquerades as the destination server. When selecting *Local Certificate*, three certificate type options appear in the *Import Certificate* pane:

<b>Local Certificate</b>	There is no field to upload a key with this option. Use this option when you have created a CSR on the FortiGate, as the key is generated as part of the CSR process and remains on the FortiGate. You will need to upload a .CER file.
<b>PKCS #12 Certificate</b>	This option takes a specific certificate file type that contains the private key. The certificate will be encrypted and a password must be supplied with the certificate file.
<b>Certificate</b>	This option is intended for certificates that were generated without using the FortiGate's CSR. Since the certificate private key is being uploaded, a password is required. This can be done two ways: <ul style="list-style-type: none"> <li>• Certificate file and key file (typically .CER and .PEM)</li> <li>• Certificate and key bundle file (typically .PFX)</li> </ul>

### CA certificate

FortiGates come with many CA certificates from well-known certificate authorities pre-installed, just as most modern operating systems like Windows and MacOS. Use this option to add private CA certificates to the FortiGate so that certificates signed by this private CA are trusted by the FortiGate.

For example, a private CA can be used when two FortiGates are establishing a site-to-site VPN tunnel using a certificate not signed by a public or trustworthy CA, or for your LDAPS connection to your corporate AD server that also uses a certificate signed with a private CA in your domain. It is very common to upload a private CA when using PKI user authentication, since most PKI user certificates will be signed by an internal CA.

When selecting *CA Certificate*, two type options appear in the *Import CA Certificate* pane:

<b>Online SCEP</b>	The FortiGate contacts an SCEP server to request the CA certificate.
<b>File</b>	The CA certificate is uploaded directly to the FortiGate.

## Remote certificate

Remote certificates are public certificates and contain only the public key. They are used to identify a remote device. For example, when configuring your FortiGate for SAML authentication with the FortiGate as an identity provider (IdP), you can optionally specify the service provider (SP) certificate. However, when configuring your FortiGate as a SP, you must specify the certificate used by the IdP. Both these certificates can be uploaded to the FortiGate as a remote certificate, since the private key is not necessary for its implementation.

## CRL

Since it is not possible to recall a certificate, the CRL (certificate revocation list) list details certificates signed by valid CAs that should no longer be trusted. Certificates may be revoked for many reasons, such as if the certificate was issued erroneously, or if the private key of a valid certificate has been compromised. When selecting *CRL*, two import methods are available:

<b>File Based</b>	CAs publish a file containing the list of certificates that should no longer be trusted.
<b>Online Updating</b>	This is the preferred way to keep the list of revoked certificates up to date. Three protocols are offered: HTTP, LDAP, and SCEP.

## Uploading a certificate using the CLI

### Generate certificate signing request

The generated CSR must be signed by a CA then loaded to the FortiGate. See [Generate certificate signing request on page 733](#) for more details.

#### To generate a CSR:

```
execute vpn certificate local generate cmp <certificate_name> <key_size> <server> <path>
<server_certificate> <auth_certificate> <user> <password> <subject> [SANs] [ip]

execute vpn certificate local generate default-ssl-ca

execute vpn certificate local generate default-ssl-key-certs

execute vpn certificate local generate default-ssl-serv-key

execute vpn certificate local generate ec <certificate_name> <curve_name> <subject>
<country> <state/province> <city> <organization> <OU> <email> [SANs] [options]

execute vpn certificate local generate rsa <certificate_name> <key_size> <subject>
<country> <state/province> <city> <organization> <OU> <email> [SANs] [options]
```

<b>cmp</b>	Generate a certificate request over CMPv2.
------------	--------------------------------------------

default-ssl-ca	Generate the default CA certificate used by SSL Inspection.
default-ssl-ca-untrusted	Generate the default untrusted CA certificate used by SSL Inspection.
default-ssl-key-certs	Generate the default RSA, DSA and ECDSA key certs for ssl resign.
default-ssl-serv-key	Generate the default server key used by SSL Inspection.
ec	Generate an elliptic curve certificate request.
rsa	Generate a RSA certificate request.

## Import

Any certificate uploaded to a VDOM is only accessible to that VDOM. Any certificate uploaded to the Global VDOM is globally accessible by all VDOMs.

A signed certificate that is created using a CSR that was generated by the FortiGate does not include a private key, and can be imported to the FortiGate from a TFTP file server.

### To import a certificate that does not require a private key:

```
execute vpn certificate local import tftp <file_name> <server_address> <cert_type>
[password]
```

### To import a certificate that requires a private key to a VDOM, or when VDOMs are disabled:

```
config vpn certificate {local | ca | remote | ocsf-server | crl}
```

Refer to the FortiOS CLI Reference for detailed options for each certificate type ([local](#), [CA](#), [remote](#), [OSCP server](#), [CRL](#)).

### To import a global certificate that requires a private key when VDOMs are enabled:

```
config certificate {local | ca | remote | crl}
```

This command is only available when VDOMs are enabled. For details, see the [FortiOS CLI Reference](#).

## Uploading a certificate using an API

There are several API methods to upload a certificate based on the type and purpose of the certificate. The parameters of each method are available options, and some methods do not require all parameters to upload the certificate.

When uploading a certificate to the FortiGate using API, the certificate must be provided to the FortiGate in Base64 encoding. You must create a REST API user to authenticate to the FortiGate and use the generated API token in the request.

### [api/v2/monitor/vpn-certificate/ca/import](#)

```
{
 "import_method": "[file|scep]",
 "scep_url": "string",
 "scep_ca_id": "string",
 "scope": "[vdom*|global]",
}
```

```
 "file_content": "string"
}
```

### **api/v2/monitor/vpn-certificate/crl/import**

```
{
 "scope": "[vdom*|global]",
 "file_content": "string"
}
```

### **api/v2/monitor/vpn-certificate/local/import**

```
{
 "type": "[local|pkcs12|regular]",
 "certname": "string",
 "password": "string",
 "key_file_content": "string",
 "scope": "[vdom*|global]",
 "acme-domain": "string",
 "acme-email": "string",
 "acme-ca-url": "string",
 "acme-rsa-key-size": 0,
 "acme-renew-window": 0,
 "file_content": "string"
}
```

### **api/v2/monitor/vpn-certificate/remote/import**

```
{
 "scope": "[vdom*|global]",
 "file_content": "string"
}
```

### **api/v2/monitor/vpn-certificate/csr/generate**

```
{
 "certname": "string",
 "subject": "string",
 "keytype": "[rsa|ec]",
 "keysize": [1024|1536|2048|4096],
 "curvename": "[secp256r1|secp384r1|secp521r1]",
 "orgunits": [
 "string"
],
 "org": "string",
 "city": "string",
 "state": "string",
 "countrycode": "string",
 "email": "string",
 "sub_alt_name": "string",
 "password": "string",
 "scep_url": "string",
 "scep_password": "string",
 "scope": "[vdom*|global]"
}
```



## Example

In this example, a PKCS 12 certificate is uploaded as a local certificate using Postman as the API client. PowerShell is used for the Base64 encoding.

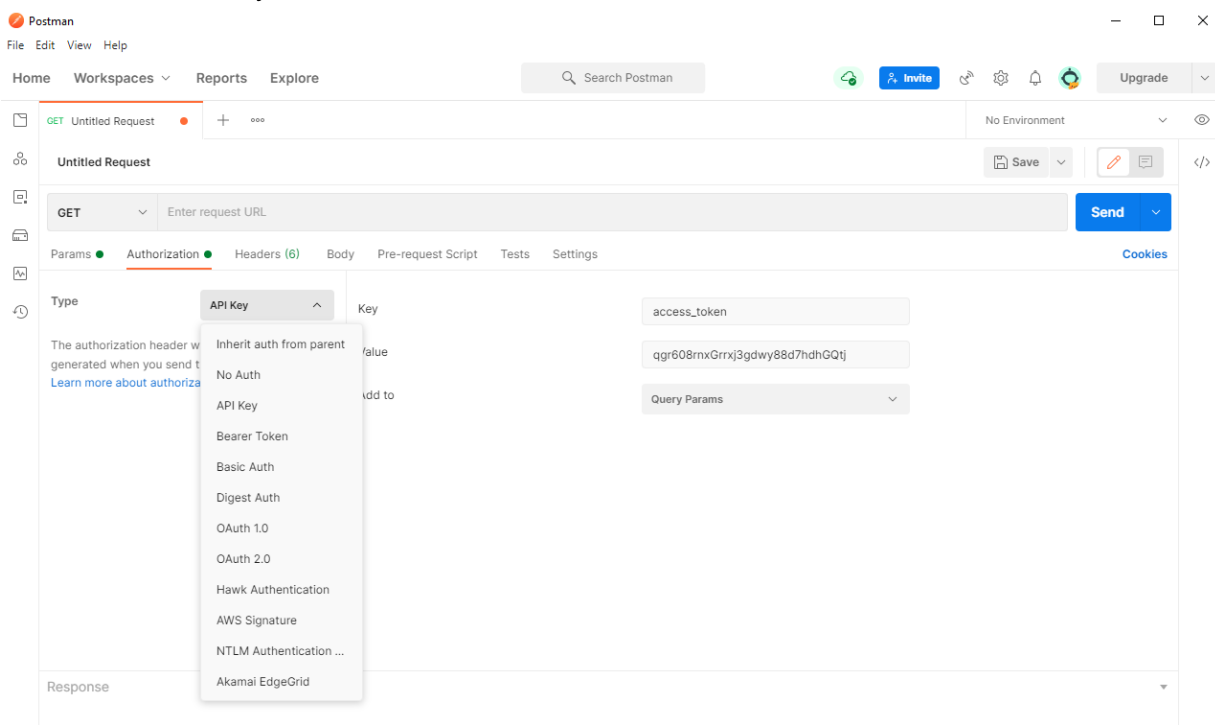
### To upload a PKCS 12 certificate using an API:

1. In PowerShell , encode the PKCS 12 certificate to Base64:

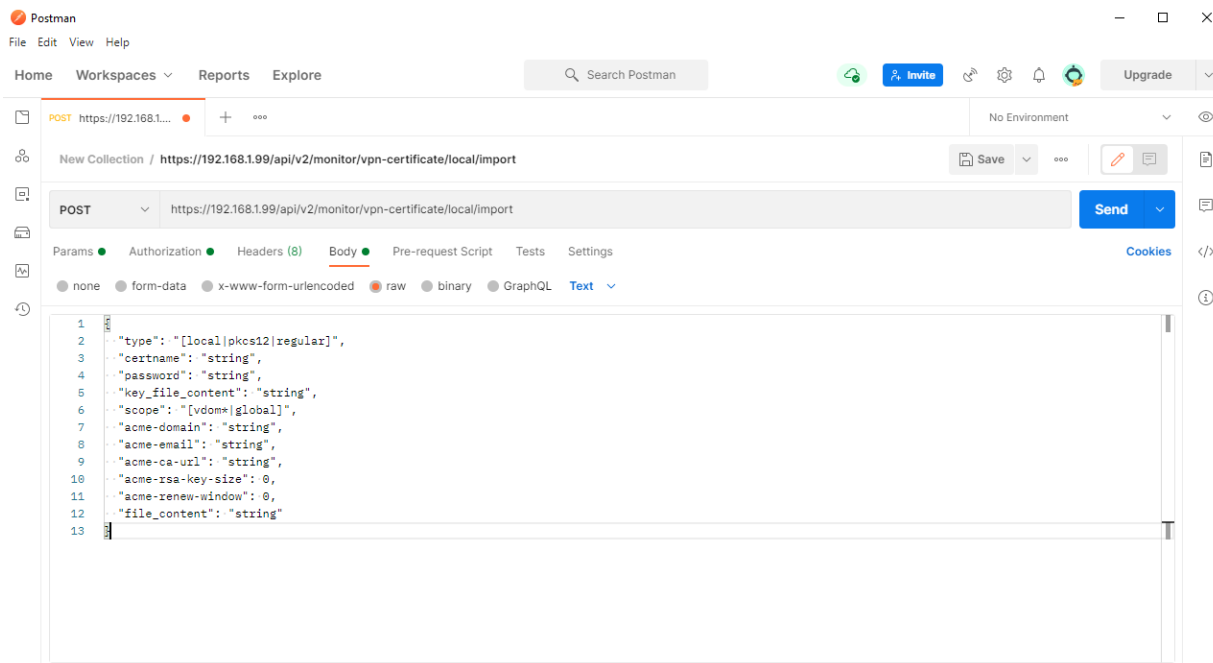
```
cd C:\users\username\desktop
$pkcs12cert = get-content 'C:\users\path\to\certificate\certificatename.p12' -Encoding
Byte
[System.Convert]::ToBase64String($pkcs12cert) | Out-File 'base12encodedcert.txt'
```

These three lines of code do the following:

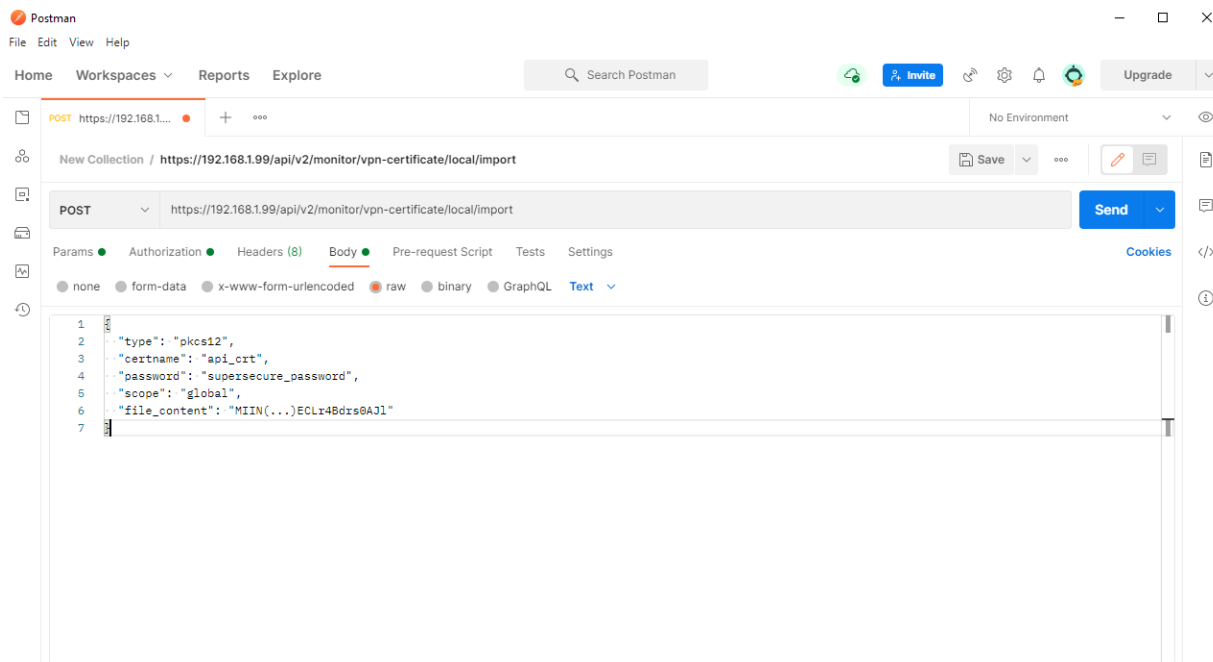
- a. Changes to working directory to the location where the encoded certificate will be created. In this example, it is the desktop.
  - b. Creates a variable called `$pkcs12cert` and defines it as the certificate file by specifying the full path to the certificate.
  - c. Creates a text file called `base12encodedcert` at the location specified in the first step. You will copy and paste the contents of this as `file_content` later in Postman.
2. Generate an API token on the FortiGate by creating a REST API user. See [Generate an API token](#) on the Fortinet Developer Network. A [subscription to the Fortinet Developer Network](#) is required to view this topic.
  3. Open Postman and create a new request:
    - a. Click the +.
    - b. Click the *Authorization* tab and in the *Type* dropdown, select *API Key*.
    - c. For *Key*, enter *access\_token* and enter the *Value* for the API user.
    - d. For *Add to*, select *Query Params*.



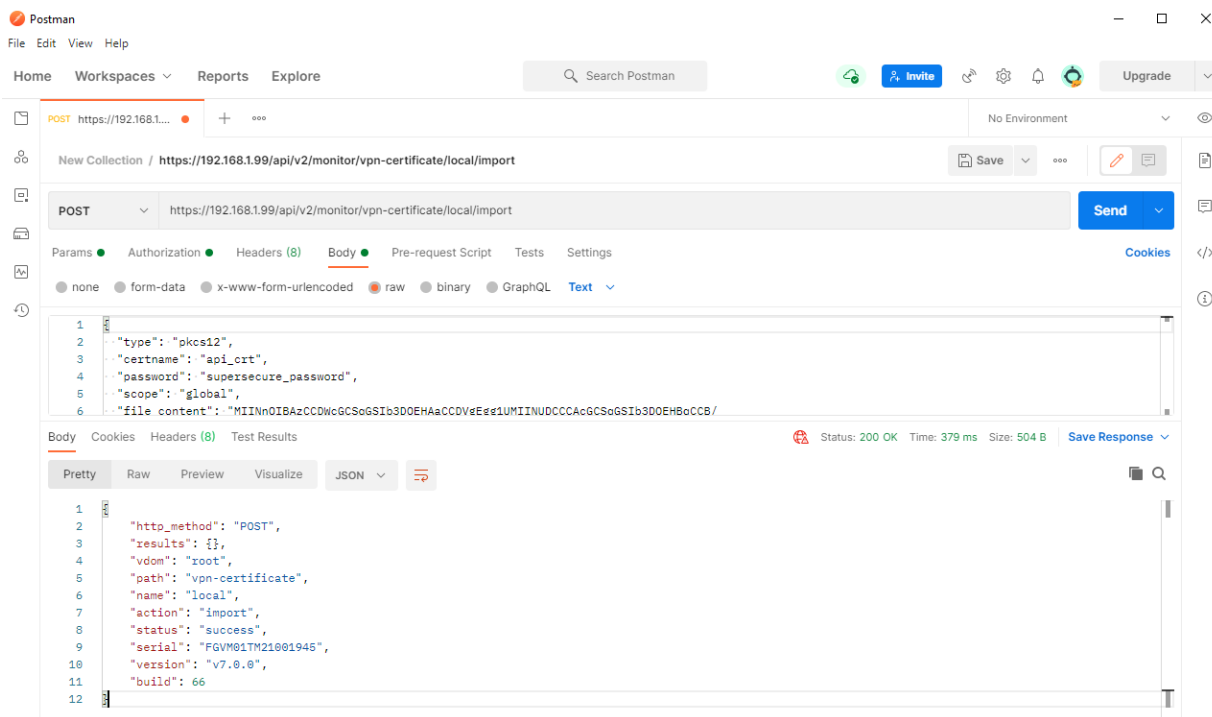
4. In the HTTP request dropdown, change the request from *GET* to *POST*, and enter the FortiGate's IP address and the URL of the API call.
5. Click the *Body* tab, and copy and paste the API parameters.



6. Remove unnecessary parameters (ACME related parameters and `key_file_content`) and enter the correct settings for your certificate. Copy and paste the contents of the file generated by PowerShell earlier into `file_content`.



7. Click **Send**. The lower window will return the results.



8. In FortiOS, go to **System > Certificates** and verify that the uploaded certificate is shown in the table (*api\_crt*).

### To debug using the HTTPS daemon:

```
diagnose debug reset
diagnose debug enable
diagnose debug application httpsd -1
<output>
diagnose debug disable
```

## Procure and import a signed SSL certificate

A signed SSL certificate can be used when configuring SSL VPN, for administrator GUI access, and for other functions that require a certificate.



Before creating a certificate, you must have a registered domain. With a valid FortiGuard subscription, FortiDDNS can be used to register a domain; see DDNS for more information.

Follow these instructions to purchase, import, and use a signed SSL certificate:

- Obtain, setup, and download an SSL certificate package from a certificate authority
- Generate a CSR
- Import the signed certificate into your FortiGate
- Configure your FortiGate device to use the signed certificate

## Obtain, setup, and download an SSL certificate package from a certificate authority

SSL certificate packages can be purchased from any Certificate Authority (CA), such as [DigiCert](#), [GoDaddy](#), or [GlobalSign](#).



[Let's Encrypt](#) can be used to generate a free, trusted SSL certificate. See [Provision a trusted certificate with Let's Encrypt on page 750](#) for details.



A third party CA might not sign a certificate with an intranet name or IP address. For details, see [Can I request a certificate for an intranet name or IP address?](#)

---

The process for purchasing, setting up, and downloading a certificate will vary depending on the CA that is used, and if a CSR must be generated on the FortiGate.

### To purchase a certificate package:

1. Create an account with your chosen vendor, or use the account that you used to purchase your domain.
2. Locate the SSL Certificates page.
3. Purchase a basic SSL certificate for domain validation only. If required, a more secure SSL certificate can be purchased.
4. If required, load the CSR, either by uploading the text file or copying and pasting the contents into the requisite text box. See [Generate a CSR on page 742](#) for information on generating the CSR on the FortiGate.
5. If required, set the server type to *Other*.
6. Verify the certificate per the requirements of the CA.
7. Download the signed certificate to your computer.
8. Import the signed certificate into your FortiGate; see [Import the signed certificate into your FortiGate on page 744](#).

## Generate a CSR

Some CAs can auto-generate the CSR during the signing process, or provide tools for creating CSRs. If necessary, a CSR can be created in your FortiGate device's GUI.

### To generate a CSR on your FortiGate:

1. Go to *System > Certificates*. By default, the *Certificate* option is not visible, see [Feature visibility on page 732](#) for information.

2. Click **Generate**. The **Generate Certificate Signing Request** page opens.

3. Configure the CSR request:

- Ensure that the certificate has a unique name.
- Set the *ID Type* to *Domain Name* and enter a *Domain Name*.
- An email address is required.
- Ensure that the *Key Size* is set to *2048 Bit*.
- Set the *Enrollment Method* to *File Based*.

4. Click **OK**.

The CSR will be added to the certificate list with a status of *PENDING*.

5. In the certificate list, select the new CSR then click **Download** to save the CSR to your computer.

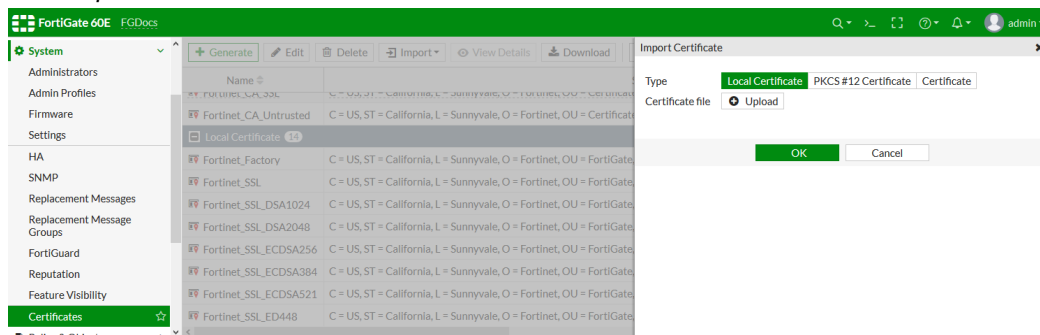
The CSR file can be opened in any text editor, and will resemble the following:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICuTCCAaECAQAwSzEcMBoGA1UEAxMTZm9ydG1zc2x2cG5kZW1vLmNvbTlrc2x2cG5kZW1vLmNvbTCCASIdDQYJ
KoZIHvcNAQEBBQADgGEPADCCAQoCggEBAMtnpNoR20NH2+UEX/NsyCmZhQqc4af3
Belu9iOoNbo9Fk42gw47r71moAN+1jTL/Tcp3hRhXtpgoI7Zh3vjZnBbD2wwU8Ow
U7dlh5MULyMehR9r4T6OAJl4KbkPt5u90r5SpIb6mM10IKvzMncuRS66rW1St0KP
mp/f6QjppjMrthnyJkCeJgyTA1YwWNuT9BcO6PTkxBqVMLaRP6TUH6He9uhOx1Cj/
5tzvSdAozZIr2moMieQy0lNd6oQcgpDzaB9QN41+cZ0lUXRCMPoH7E4Kue3/Gnis
+NMdQ8rIBijvWCXrKj20wb6sUEjAGJkcXlqVHWYCKWXl6Owejmc4ipkCAwEAAAp
MCcGCsGSIb3DQEJJDjEaMBgwCQYDVR0TBAlwADALBgNVHQ8EBAMCBaAwDQYJKoZI
hvcNAQELBQADgGEBAAJKhztz2BPIKEHH9HcJKnfBKL+a6vu1l+1sW+YqnyD+3oR9ec
0eCmLnPxxyxsVel/tRsUg4DTfmooLNDhOjgfMsWxAGUQgrDH2k87cw6kiDAPCqv1
b+hFPNKZQsd09+HXAvOpXrMlrw5YdSaoRnau6Q02yUIYennKTIZFIscgh1mk4FSe
mb12DhPF+QyDdCGDgtqnQbfXlDC0WmDcmxwa/0ZktoQhheEbYgJ20714TMqOxs/q
AZgwJlSNGBALLA2AxkIRUMKUteDdXz0QE8xNrvZpLTbWCNIpYJdRRqSd5C1w2VF4
CFgugTjFaJ13kYmBimeMRQsFtjLV5AxN+bUUsnQ=
-----END CERTIFICATE REQUEST-----
```

## Import the signed certificate into your FortiGate

To import the signed certificate into your FortiGate:

1. Unzip the file downloaded from the CA.  
There should be two CRT files: a CA certificate with *bundle* in the file name, and a local certificate.
2. Log in to your FortiGate unit and go to *System > Certificates*.
3. Click *Import > Local Certificate*.



4. Upload the local certificate file, then click *OK*.
5. The status of the certificate will change from *PENDING* to *OK*.
6. Click *Import > CA Certificate*.
7. Set the *Type* to *File*, upload the CA certificate file, then click *OK*.  
The CA certificate will be listed in the *CA Certificates* section of the certificates list.

## Configure your FortiGate device to use the signed certificate

After the signed certificates have been imported, you can use it when configuring SSL VPN, for administrator GUI access, and for other functions that require a certificate.

To configure your FortiGate to use the signed certificate for SSL VPN:

1. Go to *VPN > SSL-VPN Settings*.
2. Set *Server Certificate* to the new certificate.
3. Configure other settings as needed.
4. Click *Apply*.

For more information on configuring SSL VPN, see [SSL VPN on page 1370](#) and the [Setup SSL VPN](#) video in the Fortinet Video Library.

To configure using the certificate for administrator GUI access in the CLI:

```
config system global
 set admin-server-cert fortisslvpndemo
end
```

To change the certificate that is used for administrator GUI access in the GUI:

1. Go to *System > Settings*.
2. In the *Administration Settings* section, change *HTTPS server certificate* as needed.

3. Click *Apply*. You will be logged out of FortiOS.

## Microsoft CA deep packet inspection

In most production environments, you want to use a certificate issued by your own PKI for deep packet inspection (DPI).

An existing Microsoft root CA can be used to issue a subordinate CA (sub CA) certificate that is installed as a DPI certificate on the FortiGate.

Complete the following steps to create your own sub CA certificate and use it for DPI:

1. [Create a Microsoft sub CA certificate](#)
2. [Export the certificate and private key](#)
3. [Import the certificate and private key into the FortiGate](#)
4. [Configure a firewall policy for DPI](#)
5. [Verify that the sub CA certificate is being used for DPI](#)

The FortiGate firewall uses information in the original web server certificate, then issues a new certificate signed by the Microsoft DPI certificate. The FortiGate then sends this certificate with the issuing DPI certificate to the client's web browser when the SSL session is being established.

The browser verifies that the certificate was issued by a valid CA, then looks for the issuing CA of the Microsoft DPI certificate in its local trusted root CA store to complete the path to trusted root CA.

The Microsoft CA root certificate is normally deployed to all client PCs in the Windows domain, so the client can complete the certificate path up to a trusted root CA. The FortiGate now controls and can inspect the two HTTPS sessions: one with the external web server, and one with the client PC.

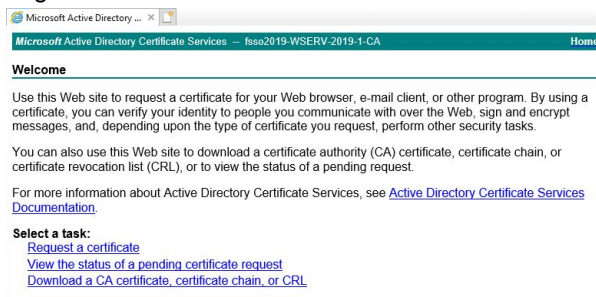
### Create a Microsoft sub CA certificate

A Microsoft sub CA certificate can be created on a Microsoft CA server, or remotely using a web browser.

Creating a certificate remotely requires that the web enrollment option is configured on the Microsoft CA server. Remote certificate requests require HTTPS; requests are not allowed with HTTP.

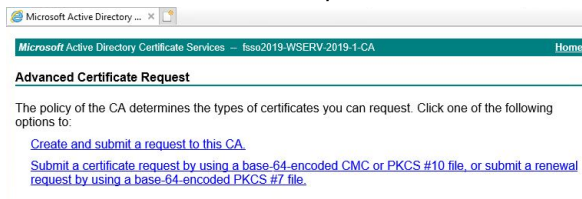
#### To create a Microsoft sub CA certificate remotely:

1. Open a web browser and go to one of the following URLs:
  - <https://<FQDN-CA-server>/CertSrv>
  - <https://<IP-CA-server>/CertSrv>.
2. Log in to a domain administrator account that has web enrollment rights.



3. Click *Request a certificate*.

#### 4. Click *advanced certificate request*.



#### 5. Click *Create and submit a request to this CA*, then click *Yes* in the *Web Access Confirmation* warning.

#### 6. For the *Certificate Template*, select *Subordinate Certification Authority*.

#### 7. Enable *Mark keys as exportable*.

#### 8. Fill out the remaining information according to your security policy.

#### 9. Submit the request.

#### 10. Click *Yes* in the *Web Access Confirmation* warning.

#### 11. Click *Install this certificate*.

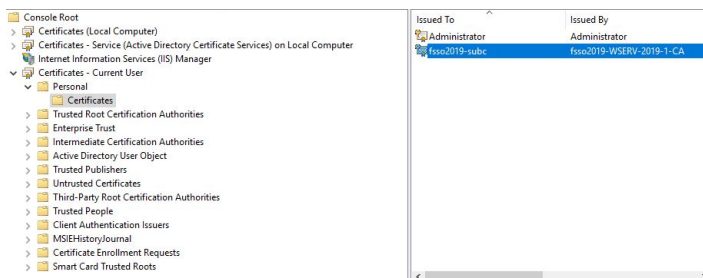
The certificate and private key are located in the current user's certificate store.

## Export the certificate and private key

### To export the certificate and private key:

#### 1. Open the Microsoft Management Console (MMC) and add the *Certificate Snap-in*.

#### 2. Go to the user's certificate store to locate the sub CA certificate that you just installed.



#### 3. Right-click on the certificate and select *All Tasks > Export*.

#### 4. Click *Next* to start the *Microsoft Certificate Export Wizard*.



5. Follow the steps in the wizard:

- When asked, select *Yes, export the private key*.
- Only the PKCS #12 (.PFX) format is available, and it requires a password.
- When selecting the encryption type, select *TripleDES-SHA1* if you are using an older version of FortiOS (5.6.9 and earlier). Otherwise, select *AES256-SHA256*.

6. Complete the wizard, and save the DPI certificate to a local folder.

## Import the certificate and private key into the FortiGate

The certificate can be imported from the local computer using the GUI, or from a TFTP server using the CLI.

After importing the certificate, you can view it in the GUI to verify that it was successfully imported.

### To import the certificate and private key into the FortiGate in the GUI:

1. Go to *System > Certificates*.
2. Select *Import > Local Certificate*.
3. Set *Type* to *PKCS #12 Certificate*.
4. Click *Upload* and locate the certificate file.
5. Enter the *Password*.
6. Optionally, modify the *Certificate Name*.

7. Click *OK*.

### To import the certificate and private key into the FortiGate in the CLI:

```
execute vpn certificate local import <certificate file name> <tftp ip address> <password>
```

## To verify that the certificate was imported:

1. Go to *System > Certificates*.
2. Locate the newly imported certificate in the table.
3. Select the certificate and click *View Details* to view the certificate details.

**FortiGate 200D** FG200D3913807264

**Certificates**

Name	Subject
Fortinet_Factory	C = US, CN = FG200D3913807264, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com
Fortinet_SSL	C = US, CN = FG200D3913807264, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com
Fortinet_SSL_DSA1024	C = US, CN = FG200D3913807264, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com
Fortinet_SSL_DSA2048	C = US, CN = FG200D3913807264, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com
Fortinet_SSL_ECDSA256	C = US, CN = FG200D3913807264, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com
Fortinet_SSL_ECDSA384	C = US, CN = FG200D3913807264, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com
Fortinet_SSL_RSA1024	C = US, CN = FG200D3913807264, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com
Fortinet_SSL_RSA2048	C = US, CN = FG200D3913807264, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com
Fortinet_WiFi	C = US, CN = auth-cert.fortinet.com, L = Sunnyvale, O = Fortinet, Inc., ST = California, OU = FortiWiFi
Local CA Certificates (2)	
Fortinet_CA_SSL	C = US, CN = FG200D3913807264, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com
Fortinet_CA_Untrusted	C = US, CN = Fortinet Untrusted CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com
fso2019subca-AES256	C = CA, CN = fso2019-subc, L = Burnaby, O = MyCompany, ST = BC, emailAddress = support@fso2019.com
Import CA Certificates (1)	
Fortinet_CA	C = US, CN = support, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com
Fortinet_WiFi_CA	C = US, OU = www.digicert.com, O = DigiCert Inc, CN = DigiCert SHA2 High Assurance Server CA
G_CA_Cert_1	C = CA, CN = Eternity-CA, L = Burnaby, O = Fortinet, ST = BC, OU = QA
Certificate Revocation (1)	
G_CRL_1	

**Certificate Detail Information**

**fso2019subca-AES256**  
Serial Number: 2A000000000000000000000000000004

**Subject Information**

Common Name (CN): fso2019-subc  
Organization (O): MyCompany  
Locality (L): Burnaby  
State (ST): BC  
Country/Region (C): CA  
Email Address: support@fso2019.com

**Issuer**

Common Name (CN): fso2019-WSERV-2019-1-CA

**Validity Period**

Valid From: 2019/07/31 13:18:27  
Valid To: 2021/07/31 13:28:27

**Fingerprints**

MD5 Fingerprint: A1:36:36:B3:A1:36:36:BB:36:36:AC:BD:36:36

**Extension**

X509v3 Key Usage: Digital Signature, Certificate Sign, CRL Sign  
OID enroll certtype extension: Microsoft specific extension: SsubCA  
X509v3 Subject Key Identifier: 72:AB:AB:9E:E5:AB:7F:E7:61:27:2C:B7:1D:D4:57:57:57:57  
X509v3 Authority Key Identifier: keyId:EF:0B:F2:71:D8:95:24:27:DF:69:8B:64:C8:23:23:23:23:23  
X509v3 CRL Distribution Points: Full Name: URIIdap://CN=fso2019-WSERV-2019-1-CA,CN=Wserv-2019-1,CN=CDPCN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=fso2019,DC=com/certific  
Authority Information Access: CA Issuers - URIIdap://CN=fso2019-WSERV-2019-1-CA,CN=Wserv-2019-1,CN=CDPCN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=fso2019,DC=com/certific  
X509v3 Basic Constraints: CA:TRUE

Close

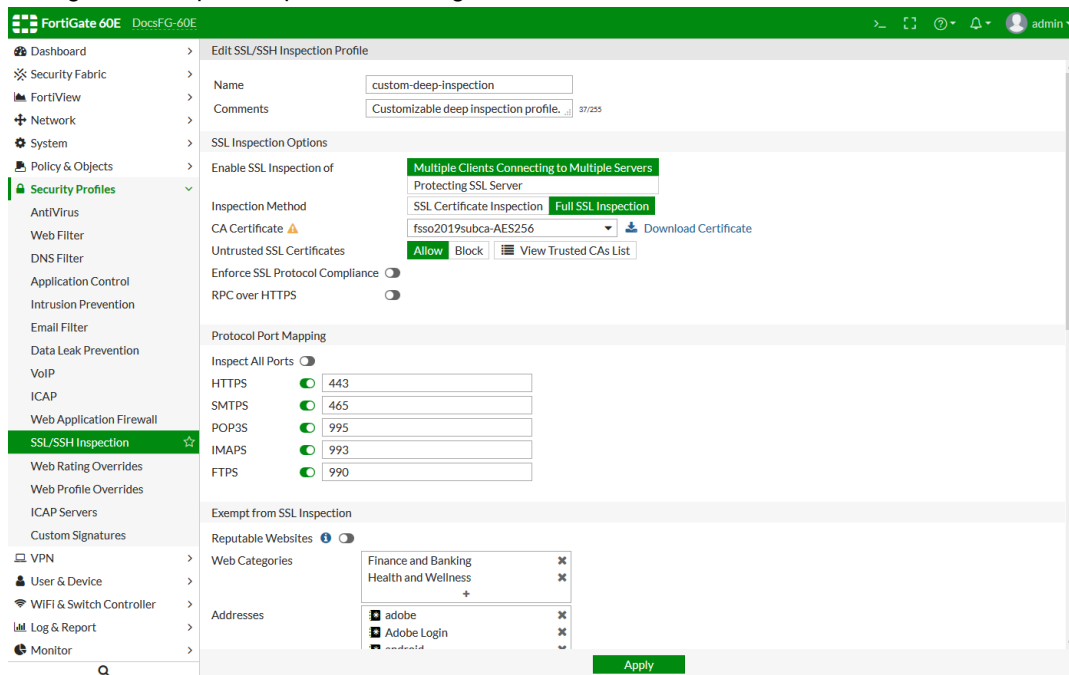
## Configure a firewall policy for DPI

The certificate is used in an SSL/SSH inspection profile that is then used in a firewall policy.

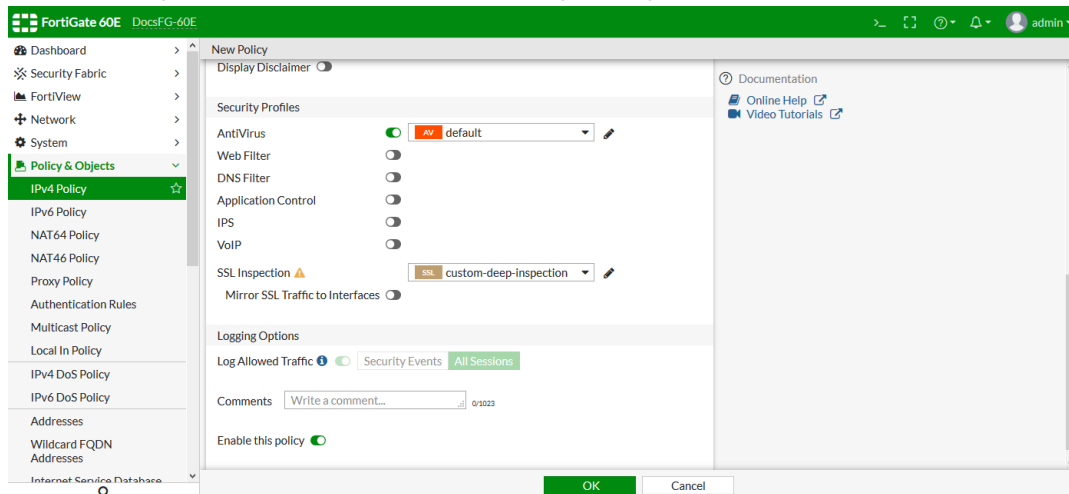
### To configure a firewall policy for DPI:

1. Go to *Security Profiles > SSL/SSH Inspection*.
2. Click *Create New*.

### 3. Configure the inspection profile, selecting the new certificate



4. Click *Apply*.
5. Go to *Policy & Objects > IPv4 Policy*.
6. Create a new policy, or edit an existing policy.
7. In the *SSL Inspection* field, select the new SSL inspection profile.



8. Configure the remaining settings as needed.
9. Click *OK*.

## Verify that the sub CA certificate is being used for DPI

You can verify that the certificate is being used for resigning web server certificates when a user connects to an external HTTPS website.

**To verify that the certificate is being used:**

1. On a client PC that is behind the FortiGate, go to an external HTTPS website.  
When connecting to the website, no certificate warning should be shown.
2. In your web browser, view the certificate and certificate path.  
The methods for doing this vary depending on the browser. See your browsers documentation for information.

## Provision a trusted certificate with Let's Encrypt

Let's Encrypt can be used to generate a free, trusted certificate that can be used by FortiGate to establish valid SSL connections that do not generate certificate warnings. See the [Let's Encrypt documentation](#) for more information and different methods of generating a trusted certificate.



Let's Encrypt certificates have 90 day lifespans. They recommend replacing the certificate every 60 days.

---

The main requirements for using Let's Encrypt are:

- An FQDN that is publicly resolvable to an IP address that you own.
- Proof of ownership of the domain.
- An application that uses Automatic Certificate Management Environment (ACME) to generate the certificate.



Fortinet has a dynamic DNS service that you can use if you do not have your own domain. See [DDNS on page 357](#) for more information.

---

This example uses Certbot to satisfy proof of ownership and generation of the certificate. It is an ACME client with a built-in, temporary webserver used for proof of domain ownership. Follow the instructions on the [Certbot website](#) to install the correct version in your Linux environment; this example uses Debian.

The Certbot application must be reachable by Let's Encrypt on TCP port 80 on the IP address that your FQDN resolves to.

## Configure your FortiGate to reach the Linux environment

You can use a VIP to forward requests to your Linux environment on port 80. In this example, the Linux environment has the IP address 10.100.80.200.

**To create a VIP to forward requests to your Linux environment on port 80 in the GUI:**

1. Go to *Policy & Objects* > *Virtual IPs* and click *Create New* > *Virtual IP*.
2. Enter a name for the VIP and set the interface.
3. Set the *Mapped IP address/range* to the IP address of the Linux environment, in this case *10.100.80.20*.

4. Enable *Port Forwarding*, set *Protocol* to *TCP*, and set *External service port* and *Map to port* to *80*.

5. Click *OK*.

**To add the VIP to a policy to allow traffic to reach your Linux environment in the GUI:**

1. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
2. Set *Incoming Interface* to the interface used in the VIP.
3. Set *Destination* to the VIP, in this example: *Linux VM*.
4. Configure the remaining settings as required.

5. Click *OK*.

**To create a VIP and add it to a policy in the CLI:**

```
config firewall vip
 edit "Linux VM"
 set mappedip "10.100.80.200"
 set extintf "wan1"
 set portforward enable
 set extport 80
 set mappedport 80
 next
end
```

```
config firewall policy
 edit 2
 set name "To_Linux_VM"
 set srcintf "wan1"
 set dstintf "internal5"
 set srcaddr "all"
 set dstaddr "Linux VM"
 set action accept
 set schedule "always"
 set service "ALL"
 set logtraffic all
 set nat enable
 next
end
```

## Create and upload the certificate

### To manually request a certificate:

1. In the Linux command line enter:

```
certbot certonly
```

```
How would you like to authenticate with the ACME CA?
```

```

```

```
1: Spin up a temporary webserver (standalone)
```

```
2: Place files in webroot directory (webroot)
```

2. Press 1 to load a temporary webserver.

```
Please enter in your domain name(s) (comma and/or space separated) (Enter 'c' to
cancel):
```

3. Enter your FQDN, such as `company.domain.com`.

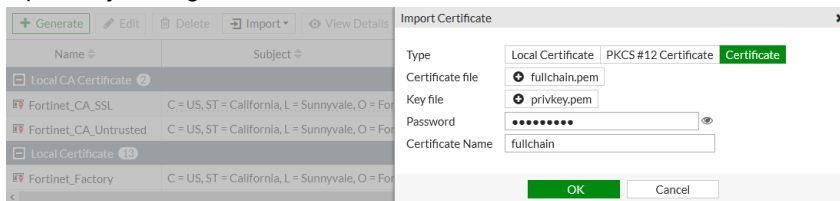
Four files should be generated:

- `cert.pem`
- `chain.pem`
- `fullchain.pem`
- `privkey.pem`

### To import the certificate and private key into the FortiGate in the GUI:

1. Go to *System > Certificates*. By default, the *Certificates* option is not visible, see [Feature visibility on page 732](#) for information.
2. Click *Import > Local Certificate*.
3. Set *Type* to *Certificate*.
4. For *Certificate File*, upload the *fullchain.pem* file.
5. For *Key File*, upload the *privkey.pem* file.
6. Enter a password.

## 7. Optionally, change the *Certificate Name*.



## 8. Click **OK**.

## Configure your FortiGate to use the signed certificate

After the signed certificates have been imported, you can use it when configuring SSL VPN and for administrator GUI access.

### To configure your FortiGate to use the signed certificate for SSL VPN:

1. Go to **VPN > SSL-VPN Settings**.
2. Set **Server Certificate** to the new certificate.
3. Configure other settings as needed.
4. Click **Apply**.

For more information on configuring SSL VPN, see [SSL VPN on page 1370](#) and the [Setup SSL VPN](#) video in the Fortinet Video Library.

### To configure using the certificate for administrator GUI access in the CLI:

```
config system global
 set admin-server-cert fullchain
end
```

### To change the certificate that is used for administrator GUI access in the GUI:

1. Go to **System > Settings**.
2. In the **Administration Settings** section, change **HTTPS server certificate** as needed.
3. Click **Apply**. You will be logged out of FortiOS.

## Creating certificates with XCA

This topic explains how to generate various certificates to be used in conjunction with a FortiGate, including:

- CA certificate
  - Signing server and client certificates
  - Issuing subordinate CAs for deep inspection
- Server certificate
  - SSL/TLS web administration authentication
  - VPN authentication
  - Internal SSL server protection
- Client certificate
  - End user authentication for SSL or IPsec VPN

XCA is an x509 certificate generation tool that handles RSA, DSA, and EC keys, as well as certificate signing requests (PKCS #10) and CRLs.



There are several options for generating and managing certificates. This topic covers basic certificate generation for XCA. It is not a comprehensive guide to its application and does not explore all options available when generating a certificate.

---

## Creating the XCA database

Before creating any certificates, you must create an XCA database to group the certificates in. You should use a different database for each PKI you create.

### To create the database:

1. Go to *File > New Database*.
2. Select a directory to store the created certificates and keys.
3. Enter a name. The provided password encrypts the private keys and is used to access the XCA database in the future.

The remaining procedures in this topic assume you are using this XCA database.

## Creating a CA certificate

A CA certificate marks the root of a certificate chain. If this CA certificate is trusted by an end entity, any certificates signed by the CA certificate are also trusted.



**To create a CA certificate:**

1. Click the *Certificates* tab, then click *New Certificate*.
2. Edit the *Source* tab:
  - a. Set *Template for the new certificate* to *[default] CA*.
  - b. Click *Apply extensions*.

The screenshot shows the 'Create x509 Certificate' dialog box with the following settings:

- Signing request:**
  - ☐ Sign this Certificate signing request
  - ☒ Copy extensions from the request
  - ☐ Modify subject of the request
- Signing:**
  - ☒ Create a self signed certificate
  - ☐ Use this Certificate for signing
- Signature algorithm:** SHA 256
- Template for the new certificate:** [default] CA

Buttons at the bottom: OK, Cancel, Help. Buttons at the bottom right: Apply extensions, Apply subject, Apply all.

3. Edit the *Subject* tab:
  - a. Enter an *Internal Name* to reference this certificate within XCA.
  - b. Enter a *commonName*.
  - c. Optionally, click *Add* to add other distinguished name fields.
  - d. Since this XCA database does not contain any keys yet, click *Generate a new key*. The *Private key* field is now

populated.

The screenshot shows the 'Create x509 Certificate' window with the 'Subject' tab active. The 'Distinguished name' section contains the following fields: countryName (US), stateOrProvinceName (PA), localityName (Scranton), organizationalUnitName (empty), commonName (VF\_CA), and emailAddress (empty). The 'Private key' section shows a dropdown menu with 'VF\_CA (RSA:4096 bit)' selected, and a checkbox for 'Used keys too' which is unchecked. There is a 'Generate a new key' button next to the dropdown. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

4. Optionally, edit the *Extensions* tab:
  - a. Adjust the *Time range* if needed.
  - b. Click *Apply*.
5. Click *OK*.

## Issuing a subordinate CA certificate for deep inspection

Subordinate CA certificates are similar to CA certificates because they are used to sign other certificates to establish trust of the signed certificate's content. This trust of the signed certificate is only valid if the subordinate CA is also trusted by the client.

When performing deep inspection on a FortiGate, the FortiGate proxies the connection between the endpoint and the server. This is done transparently so that the end user believes they are communicating with the server, and the server with the client. To do this, when the webpage is requested by a client, the FortiGate must present a certificate that matches the requested website and is trusted by the client.

The certificate presented by the FortiGate is generated on-demand to match the requested website and is signed by this subordinate CA to establish trust with the requesting endpoint. The subordinate CA must be installed on the FortiGate (with the private key) and on the client device (without the private key).

A subordinate CA is used in place of a CA so that it may be revoked as necessary. This is critical since the subordinate CA's private key is exported and becomes susceptible of being compromised. If the CA private key becomes compromised, you would be forced to re-create your entire PKI with a new root CA because root CAs cannot be revoked. See [Microsoft CA deep packet inspection on page 745](#) for more information about using subordinate CA certificates.

### To issue a subordinate CA certificate for deep inspection:

1. Click the *Certificates* tab, then click *New Certificate*.
2. Edit the *Source* tab:
  - a. Set *Use this Certificate for signing* to the CA created previously.
  - b. Set *Template for the new certificate* to *[default] CA*.
  - c. Click *Apply extensions*.
3. Edit the *Subject* tab:
  - a. Enter an *Internal Name* to reference this certificate within XCA.
  - b. Enter a *commonName*.
  - c. Optionally, click *Add* to add other distinguished name fields.
  - d. Click *Generate a new key* to create a new private key for the subordinate CA.

The screenshot shows the 'Create x509 Certificate' dialog box with the 'Subject' tab selected. The 'Internal Name' field contains 'VF\_sub\_CA'. The 'Distinguished name' section has the following values: countryName: US, stateOrProvinceName: PA, localityName: Scranton, and commonName: VF\_sub\_CA. The 'Private key' section shows 'VF\_sub\_CA (RSA:2048 bit)' selected, with a 'Generate a new key' button next to it. The 'Add' and 'Delete' buttons are also visible in the 'Distinguished name' section.

4. Optionally, edit the *Extensions* tab:
  - a. Adjust the *Time range* if needed.
  - b. Click *Apply*.
5. Click *OK*.

## Creating a server host certificate

When a CA signs a host certificate, that CA is vouching for the credentials in the certificate. These credentials are what identifies the host.

Some endpoints can generate a certificate signing request (CSR). A CSR is a certificate outline that specifies the details of the endpoint, including its public key. This allows the CA to review the details and sign the request if they are true. This request is then returned or uploaded to the generating endpoint to be used.

Since some endpoints cannot generate their own CSR, you can create the certificate manually in XCA. If you already have a CSR, use the *Certificate signing requests* tab to import and then sign it.

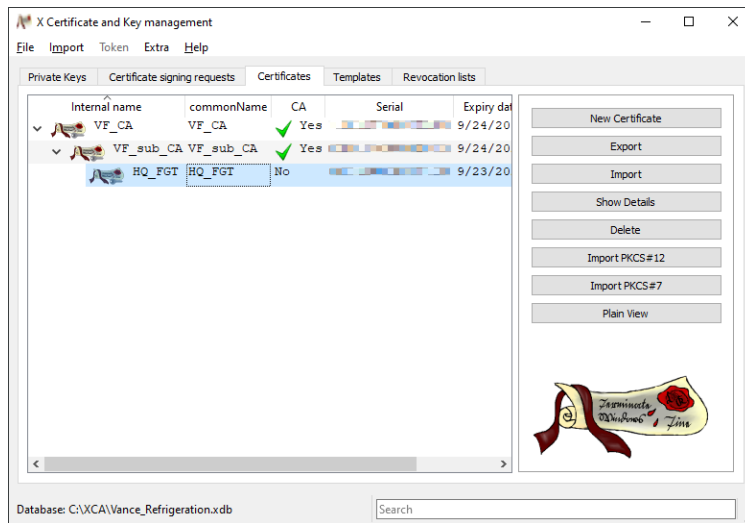
**To create a server host certificate:**

1. Click the *Certificates* tab, then click *New Certificate*.
2. Edit the *Source* tab:
  - a. Set *Template for the new certificate* to *[default] TLS\_server*.
  - b. Click *Apply extensions*.
  - c. In the *Signing* section, select *Use this Certificate for signing* and select the subordinate CA certificate.
3. Edit the *Subject* tab:
  - a. Enter an *Internal Name* to reference this certificate within XCA.
  - b. Enter the distinguished name fields as needed.
  - c. Click *Generate a new key*.

The screenshot shows the 'Create x509 Certificate' dialog box with the 'Subject' tab selected. The 'Internal Name' field contains 'HQ\_FGT'. The 'Distinguished name' section includes fields for 'countryName' (US), 'stateOrProvinceName' (PA), 'commonName' (HQ\_FGT), 'localityName' (Scranton), and 'organizationName'. The 'Private key' section shows 'HQ\_FGT (RSA:2048 bit)' selected, with a 'Generate a new key' button. The 'Add' and 'Delete' buttons are also visible.

4. Edit the *Extensions* tab:
  - a. For *X509v3 Subject Alternative Name*, enter *email:user@domain.tld*.
5. Click *OK*.

6. Click the *Certificates* tab to view the certificate.



This certificate may be used to identify an SSL or TLS server by uploading the certificate and key pair to the server, such as when the FortiGate presents the administrative webpage or for SSL VPN authentication (see [Configure your FortiGate device to use the signed certificate on page 744](#)). Another use case for a server host certificate is to enable SSL server protection so the FortiGate simulates the real server and brokers the connection (see [Protecting an SSL server on page 1096](#)).

## Creating a client host certificate

A client host certificate is used to identify an end entity in a more secure way than a username and password. Once the client host certificate is generated, see [SSL VPN with certificate authentication on page 1450](#) for more information about using the certificate.

### To create a client host certificate:

1. Click the *Certificates* tab, then click *New Certificate*.
2. Edit the *Source* tab:
  - a. In the *Signing* section, select *Use this Certificate for signing* and select the CA or subordinate CA.
  - b. Set *Template for the new certificate* to *[default] TLS\_client*.
  - c. Click *Apply extensions*.
3. Edit the *Subject* tab:
  - a. Enter an *Internal Name* to reference this certificate within XCA.
  - b. Enter the distinguished name fields as needed.

- c. Click *Generate a new key*.

4. Click **OK**.
5. Click the **Certificates** tab. The FortiGate and client certificates are listed under the signing CA certificate and are ready to be exported.

6. Select a certificate and click **Export**.
7. Enter the file name and select an export format.
8. Click **OK**.

## Certificate formats

Certificate file formats indicate what is contained in the file, how it is formatted, and how it is encoded. See [Uploading a certificate using the GUI on page 733](#) for more information about which formats the FortiGate expects for a given certificate type.

## RAID

Most FortiGate devices with multiple disk drives (SSD or HDD) can be configured to use RAID.



Enabling or disabling RAID, and changing the RAID level, erases all data on the log disk and reboots the device.

### To verify that the FortiGate has multiple disks:

- List disk devices and partitions:

```
execute disk list

Disk SSD1 ref: 255 223.6GiB type: SSD [ATA INTEL SSDSC2KB24] dev: /dev/sda
 partition ref: 1 220.1GiB, 219.0GiB free mounted: Y label: LOGUSEDXA707476A dev:
/dev/sda1 start: 2048
```

```
Disk SSD2 ref: 16 223.6GiB type: SSD [ATA INTEL SSDSC2KB24] dev: /dev/sdb
 partition ref: 17 62.7GiB, 62.4GiB free mounted: Y label: WANOPTXX1FEBBFA1 dev:
/dev/sdb1 start: 2048
 partition ref: 18 63.7GiB, 63.7GiB free mounted: N label: dev: /dev/sdb2 start:
133625856
 partition ref: 19 85.0GiB, 85.0GiB free mounted: N label: dev: /dev/sdb3 start:
267249664
```

- Display information about all of the disks:

```
diagnose hardware deviceinfo disk

Disk SSD1 ref: 255 223.6GiB type: SSD [ATA INTEL SSDSC2KB24] dev: /dev/sda
 partition ref: 1 220.1GiB, 219.0GiB free mounted: Y label: LOGUSEDXA707476A dev:
/dev/sda1 start: 2048

Disk SSD2 ref: 16 223.6GiB type: SSD [ATA INTEL SSDSC2KB24] dev: /dev/sdb
 partition ref: 17 62.7GiB, 62.4GiB free mounted: Y label: WANOPTXX1FEBBFA1 dev:
/dev/sdb1 start: 2048
 partition ref: 18 63.7GiB, 63.7GiB free mounted: N label: dev: /dev/sdb2 start:
133625856
 partition ref: 19 85.0GiB, 85.0GiB free mounted: N label: dev: /dev/sdb3 start:
267249664

Disk SYSTEM(boot) 14.9GiB type: SSD [ATA 16GB SATA Flash] dev: /dev/sdc
 partition 247.0MiB, 155.0MiB free mounted: N label: dev: /dev/sdc1(boot) start: 1
 partition 247.0MiB, 154.0MiB free mounted: Y label: dev: /dev/sdc2(boot) start: 524289
 partition ref: 35 14.2GiB, 14.0GiB free mounted: Y label: dev: /dev/sdc3 start:
1048577

Disk USB-6(user-usb) ref: 48 28.6GiB type: USB [SanDisk Ultra] dev: /dev/sdd
<<<<<====this info for usb disk because i have usb disk on FGT301E
 partition ref: 49 28.6GiB, 28.6GiB free mounted: Y label: dev: /dev/sdd1 start: 0

Total available disks: 4
Max SSD disks: 2 Available storage disks: 2
```

### To check the RAID status:

- RAID enabled:

```
execute disk raid status
RAID Level: Raid-1
RAID Status: OK (Background-Synchronizing) (9%)
RAID Size: 239GB

Disk 1: OK Used 228GB
Disk 2: OK Used 228GB
```

- RAID disabled:

```
execute disk raid status
RAID Level: Unavailable
RAID Status: Unavailable
RAID Size: 0GB

Disk 1: OK Not-Used 228GB
Disk 2: OK Not-Used 228GB
```

### To enable RAID:

```
execute disk raid enable
This will erase all data on the log disk, and system will reboot!
Do you want to continue? (y/n)y

Dependent storage SSD2 removed.
Dependent storage SSD1 removed.
Raid-0 created with 2 disks.

Performing raid on the requested disk(s) and rebooting, please wait.. .

Configuring raid...
- unmounting /data2 : ok
- unmounting /var/log : ok
- unmounting /usb : ok
- unmounting /var/storage/SSD2-WANOPTXX0EA0EF17 : ok

Formatting the disk...
- unmounting /usb : ok
Formatting /dev/md0 ... done

The system is going down NOW !!

Please stand by while rebooting the system.
Restarting system.
```

### To rebuild the RAID:

```
execute disk raid rebuild
```



**To rebuild the RAID to another level:****1. Check the supported RAID levels:**

```
execute disk raid rebuild-level
<RAID level> supported: Raid-0, Raid-1
```

**2. Rebuild the RAID to the required level:**

```
execute disk raid rebuild-level Raid-1
This will erase all data on the log disk, and system will reboot!
Do you want to continue? (y/n)y

Dependent storage RAID removed.
Raid-1 created with 2 disks.

Performing raid on the requested disk(s) and rebooting, please wait...

Configuring raid...
- unmounting /data2 : ok
- unmounting /var/log : ok
- unmounting /usb : ok

Formatting the disk...
- unmounting /usb : ok
Formatting /dev/md0 ... done

The system is going down NOW !!

Please stand by while rebooting the system.
Restarting system.
```

**To disable RAID:**

```
execute disk raid disable
This will erase all data on the log disk, and system will reboot!
Do you want to continue? (y/n)y

Dependent storage RAID removed.

Performing format on the requested disk(s) and rebooting, please wait...

Configuring raid...
- unmounting /data2 : ok
- unmounting /var/log : ok
- unmounting /usb : ok

Formatting the disk...
Partitioning and formatting /dev/sda label LOGUSEDX3D36836D ... done
Partitioning and formatting /dev/sdb label WANOPTXX1FE9BFA1 ...
Sending request for partno=0 start=2048 stop=133624230
Sending request for partno=1 start=133625856 stop=267248460
Sending request for partno=2 start=267249664 stop=445414150
done

The system is going down NOW !!
```

```

Please stand by while rebooting the system.
Restarting system.
FortiGate-301E (11:11-04.30.2018)
.
Reading boot image 3017355 bytes.
Initializing firewall...
System is starting...

```

## Conserve mode

Each FortiGate model has a specific amount of memory that is shared by all operations. If most or all of that memory is in use, system operations can be affected in unexpected ways. To control how FortiOS functions when the available memory is very low, FortiOS enters conserve mode. This causes functions, such as antivirus scanning, to change how they operate to reduce the functionality and conserve memory without compromising security.

Three memory thresholds can be configured:

```

config system global
 set memory-use-threshold-extreme <integer>
 set memory-use-threshold-green <integer>
 set memory-use-threshold-red <integer>
end

```

memory-use-threshold-extreme <integer>	The threshold at which memory usage is considered extreme and new sessions are dropped, in percent of total RAM (70 - 97, default = 95).
memory-use-threshold-green <integer>	The threshold at which memory usage forces the FortiGate to leave conserve mode, in percent of total RAM (70 - 97, default = 82).
memory-use-threshold-red <integer>	The threshold at which memory usage forces the FortiGate to enter conserve mode, in percent of total RAM (70 - 97, default = 88).

## Proxy inspection in conserve mode

The FortiGate's proxy-based inspection behavior while in conserve mode is configured with the antivirus failopen command.

```

config system global
 set av-failopen {pass | off | one-shot}
end

```

pass	<p>This is the default settings.</p> <p>Bypass the antivirus proxy and allow traffic to continue to its destination. Because traffic bypasses the proxy, security profiles that require the antivirus proxy are also bypassed. Security profiles that do not use the antivirus proxy continue to function normally.</p> <p>Use this setting when access is more important than security while the issue is resolved.</p>
------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

off	<p>Force the FortiGate to stop all traffic that uses the antivirus proxy. New sessions are blocked, but active sessions continue to be processed normally unless they request more memory and are then terminated.</p> <p>If a security policy is configured to use antivirus scanning, then the traffic that it permits is blocked while in conserve mode. So, a policy with only IPS scanning enabled will continue normally, but a policy with both IPS and antivirus scanning is blocked because antivirus scanning requires the antivirus proxy.</p> <p>Use this setting when security is more important than access while the issue is resolved.</p>
one-shot	Continue to bypass the antivirus proxy after the FortiGate is out of conserve mode, until the failopen setting is changed or the FortiGate is restarted.

## Flow inspection in conserve mode

The FortiGate's flow-based inspection behavior while in conserve mode is configured with the IPS failopen command.

```
config ips global
 set fail-open {enable | disable}
end
```

- When disabled (default), the IPS engine drops all new sessions that require flow-based inspection.
- When enabled, the IPS engine does not perform any scans and allows new packets.

## Diagnostics

When in conserve mode, FortiOS generates conserve mode log messages and SNMP traps, and a conserve mode banner is shown in the GUI.



### To view current information about memory conservation status:

```
diagnose hardware sysinfo conserve
memory conserve mode: on
total RAM: 997 MB
memory used: 735 MB 73% of total RAM
memory freeable: 173 MB 17% of total RAM
memory used + freeable threshold extreme: 947 MB 95% of total RAM
memory used threshold red: 877 MB 88% of total RAM
memory used threshold green: 817 MB 82% of total RAM
```

### To view logs:

1. Go to *Log & Report > System Events* in the GUI.
2. If historical FortiView is enabled, select the *Logs* tab.
3. If the GUI is unresponsive due to high memory usage, making the logs inaccessible, they can be viewed in the CLI:

```
execute log filter category 1
execute log display
```

```
1: date=2022-11-02 time=16:58:37 eventtime=1667433517502192693 tz="-0700"
logid="0100022011" type="event" subtype="system" level="critical" vd="root"
logdesc="Memory conserve mode entered" service="kernel" conserve="on" total=997 MB
used=707 MB red="877 MB" green="698 MB" msg="Kernel enters memory conserve mode"
```

### To view the crash log in the CLI:

```
diagnose debug crashlog read
```

```
1: 2022-10-27 14:22:36 service=kernel conserve=on total="997 MB" used="720 MB" red="877 MB"
2: 2022-10-27 14:22:36 green="817 MB" msg="Kernel enters memory conserve mode"
```

# Policy and Objects

## Policies

The firewall policy is the axis around which most features of the FortiGate revolve. Many firewall settings end up relating to or being associated with the firewall policies and the traffic they govern. Any traffic going through a FortiGate has to be associated with a policy. These policies are essentially discrete compartmentalized sets of instructions that control the traffic flow going through the firewall. These instructions control where the traffic goes, how it is processed, if it is processed, and whether or not it is allowed to pass through the FortiGate.

When the firewall receives a connection packet, it analyzes the source address, destination address, and service (by port number). It also registers the incoming interface, the outgoing interface it needs to use, and the time of day. Using this information, the FortiGate firewall attempts to locate a security policy that matches the packet. If a policy matches the parameters, then the FortiGate takes the required action for that policy. If it is *Accept*, the traffic is allowed to proceed to the next step. If the action is *Deny* or a match cannot be found, the traffic is not allowed to proceed.

The two basic actions at the initial connection are either *Accept* or *Deny*:

- If the action is *Accept*, the policy permits communication sessions. There may be other packet processing instructions, such as requiring authentication to use the policy or restrictions on the source and destination of the traffic.
- If the action is *Deny*, the policy blocks communication sessions, and you can optionally log the denied traffic. If no security policy matches the traffic, the packets are dropped. A *Deny* security policy is needed when it is required to log the denied traffic, also called *violation traffic*.

One other action can be associated with the policy:

- *IPsec*—this is an *Accept* action that is specifically for IPsec VPNs.

The following topics provide instructions on configuring policies:

- [Firewall policy parameters on page 768](#)
- [Profile-based NGFW vs policy-based NGFW on page 768](#)
- [NGFW policy mode application default service on page 773](#)
- [Policy views and policy lookup on page 775](#)
- [Policy with source NAT on page 776](#)
- [Policy with destination NAT on page 786](#)
- [Policy with Internet Service on page 799](#)
- [NAT64 policy and DNS64 \(DNS proxy\) on page 814](#)
- [NAT46 policy on page 818](#)
- [Local-in policies on page 821](#)
- [DoS protection on page 822](#)
- [IPv4/IPv6 access control lists on page 830](#)
- [Mirroring SSL traffic in policies on page 831](#)
- [Inspection mode per policy on page 831](#)
- [Combined IPv4 and IPv6 policy on page 834](#)
- [FortiGuard DNS filter for IPv6 policies on page 835](#)
- [OSPFv3 neighbor authentication on page 837](#)

- [Firewall anti-replay option per policy on page 839](#)
- [Enabling advanced policy options in the GUI on page 839](#)
- [Recognize anycast addresses in geo-IP blocking on page 840](#)
- [Authentication policy extensions on page 841](#)
- [NTLM extensions on page 842](#)
- [HTTP to HTTPS redirect for load balancing on page 845](#)
- [Use active directory objects directly in policies on page 847](#)
- [FortiGate Cloud / FDN communication through an explicit proxy on page 850](#)

## Firewall policy parameters

For traffic to flow through the FortiGate firewall, there must be a policy that matches its parameters:

- Incoming interface(s)
- Outgoing interface(s)
- Source address(es)
- User(s) identity
- Destination address(es)
- Internet service(s)
- Schedule
- Service

Without all six (possibly eight) of these things matching, the traffic is declined.

Traffic flow initiated from each direction requires a policy, that is, if sessions can be initiated from both directions, each direction requires a policy.

Just because packets can go from point A to point B on port X does not mean that the traffic can flow from point B to point A on port X. A policy must be configured for each direction.

When designing a policy, there is often reference to the traffic flow, but most communication is two-way so trying to determine the direction of the flow might be confusing. If traffic is HTTP web traffic, the user sends a request to the website, but most of the traffic flow will be coming from the website to the user or in both directions? For the purposes of determining the direction for a policy, the important factor is the direction of the initiating communication. The user is sending a request to the website, so this is the initial communication; the website is responding so the traffic is from the user's network to the Internet.



FortiOS does not perform a reverse-path check on reply traffic that matches an allowed session based on the IP tuple. The request traffic can be sent on one interface and the reply traffic could return on another interface.

---

## Profile-based NGFW vs policy-based NGFW

Profile-based next-generation firewall (NGFW) mode is the traditional mode where you create a profile (antivirus, web filter, and so on) and then apply the profile to a policy.

In policy-based NGFW mode, you allow applications and URL categories to be used directly in security policies, without requiring web filter or application control profiles.

In policy-based mode:

- Central NAT is always enabled. If no Central SNAT policy exists, you must create one. See [Central SNAT on page 783](#) for more information.
- Pre-match rules are defined separately from security policies, and define broader rules, such as SSL inspection and user authentication.

If your FortiGate operates in NAT mode, rather than enabling source NAT in individual NGFW policies, go to *Policy & Objects > Central SNAT* and add source NAT policies that apply to all matching traffic. In many cases, you may only need one SNAT policy for each interface pair.

The NGFW mode is set per VDOM, and it is only available when the VDOM inspection mode is flow-based. You can operate your entire FortiGate or individual VDOMs in NGFW policy mode.



Switching from profile-based to policy-based mode converts your policies to policy-based. To avoid issues, you could create a new VDOM for the policy-based mode. We recommend backing up your configuration before switching modes. See [Configuration backups on page 62](#) for information.

---

## Enabling policy-based NGFW mode

### To enable policy-based NGFW mode without VDOMs in the GUI:

1. Go to *System > Settings*.
2. In *NGFW Mode*, select *Policy-based*.
3. Click *Apply*.

### To enable policy-based NGFW mode with VDOMs in the GUI:

1. Go to *System > VDOM*.
2. Double-click a VDOM to edit the settings.
3. In *NGFW Mode*, select *Policy-based*.
4. Click *OK*.

### To enable policy-based NGFW mode without VDOMs in the CLI:

```
config system settings
 set ngfw-mode policy-based
end
```

### To enable policy-based NGFW mode with VDOMs in the CLI:

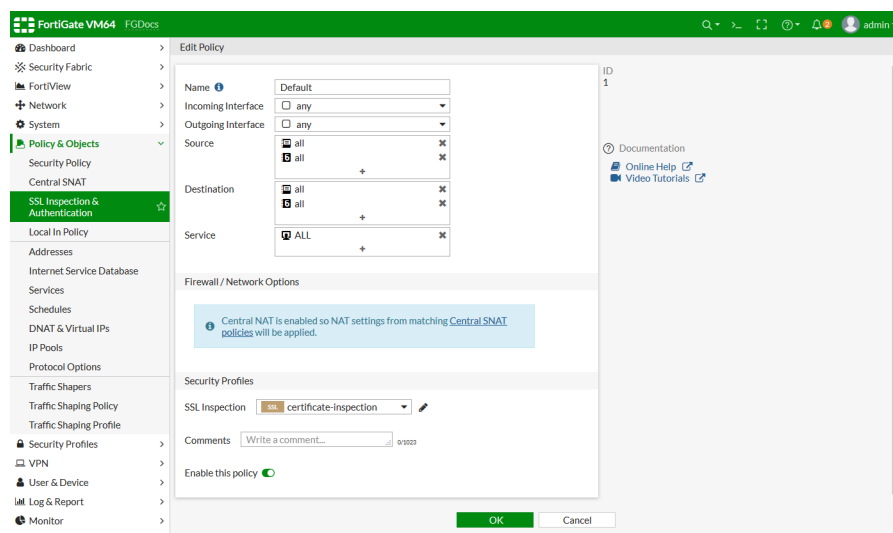
```
config vdom
 edit <vdom>
 config system settings
 set ngfw-mode policy-based
 end
 next
end
```

## Security and SSL Inspection & Authentication policies

Security policies work with SSL Inspection & Authentication policies to inspect traffic. To allow traffic from a specific user or user group, both Security and SSL Inspection & Authentication policies must be configured. A default SSL Inspection & Authentication policy with the certificate-inspection SSL Inspection profile is preconfigured. Traffic will match the SSL Inspection & Authentication policy first. If the traffic is allowed, packets are sent to the IPS engine for application, URL category, user, and user group match, and then, if enabled, UTM inspection (antivirus, IPS, DLP, and email filter) is performed.

SSL Inspection & Authentication policies are used to pre-match traffic before sending the packets to the IPS engine:

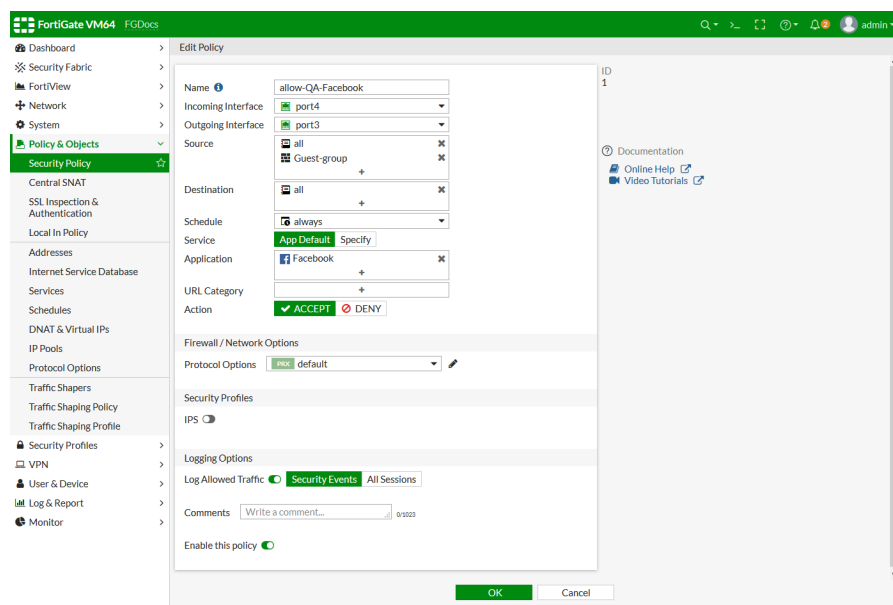
- There are no schedule or action options; traffic matching the policy is always redirected to the IPS engine.
- SSL inspection, formerly configured in the VDOM settings, is configured in an SSL Inspection & Authentication policy.
- Users and user groups that require authentication must be configured in an SSL Inspection & Authentication policy.



Security policies work with SSL Inspection & Authentication policies to inspect traffic:

- Applications and URL categories can be configured directly in the policy.
- Users and user groups that require authentication must also be configured in a security policy.
- The available actions are *Accept* or *Deny*.
- The *Service* option can be used to enforce the standard port for the selected applications. See [NGFW policy mode application default service on page 773](#) for details.
- UTM inspection is configured in a security policy.





## To configure policies for Facebook and Gmail access in the CLI:

### 1. Configure an SSL Inspection & Authentication policy:

```
config firewall consolidated policy
 edit 1
 set name "Policy-1"
 set srcintf "port18"
 set dstintf "port17"
 set srcaddr4 "all"
 set dstaddr4 "all"
 set service "ALL"
 set ssl-ssh-profile "new-deep-inspection"
 set groups "Dev" "HR" "QA" "SYS"
 next
end
```

### 2. Configure security policies:

```
config firewall security-policy
 edit 2
 set name "allow-QA-Facebook"
 set srcintf "port18"
 set dstintf "port17"
 set srcaddr4 "all"
 set dstaddr4 "all"
 set action accept
 set schedule "always"
 set application 15832
 set groups "Dev" "QA"
 next
 edit 4
 set name "allow-QA-Email"
 set srcintf "port18"
 set dstintf "port17"
 set srcaddr4 "all"
```

```
 set dstaddr4 "all"
 set action accept
 set schedule "always"
 set url-category 23
 set groups "QA"
 next
end
```

## Logs

In the application control and web filter logs, `securityid` maps to the security policy ID.

### Application control log:

```
date=2019-06-17 time=16:35:47 logid="1059028704" type="utm" subtype="app-ctrl"
eventtype="signature" level="information" vd="vd1" eventtime=1560814547702405829 tz="-0700"
appid=15832 user="Jack" group="QA" srcip=10.1.100.102 dstip=157.240.3.29 srcport=56572
dstport=443 srcintf="port18" srcintfrole="undefined" dstintf="port17"
dstintfrole="undefined" proto=6 service="P2P" direction="incoming" policyid=1
sessionid=42445 appcat="Social.Media" app="Facebook" action="pass" hostname="external-seal-
1.xx.fbcdn.net" incidentserialno=1419629662 url="/" securityid=2 msg="Social.Media:
Facebook," apprisk="medium" scertcname="*.facebook.com" scertissuer="DigiCert SHA2 High
Assurance Server CA"
```

### Web filter log:

```
date=2019-06-17 time=16:42:41 logid="0317013312" type="utm" subtype="webfilter"
eventtype="ftgd_allow" level="notice" vd="vd1" eventtime=1560814961418114836 tz="-0700"
policyid=4 sessionid=43201 user="Jack" group="QA" srcip=10.1.100.102 srcport=56668
srcintf="port18" srcintfrole="undefined" dstip=172.217.3.165 dstport=443 dstintf="port17"
dstintfrole="undefined" proto=6 service="HTTPS" hostname="mail.google.com"
action="passthrough" reqtype="direct" url="/" sentbyte=709 rcvdbyte=0 direction="outgoing"
msg="URL belongs to an allowed category in policy" method="domain" cat=23 catdesc="Web-based
Email" securityid=4
```

### Traffic logs:

```
date=2019-06-17 time=16:35:53 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="vd1" eventtime=1560814553778525154 tz="-0700" srcip=10.1.100.102
srcport=56572 srcintf="port18" srcintfrole="undefined" dstip=157.240.3.29 dstport=443
dstintf="port17" dstintfrole="undefined" poluid="b740d418-8ed3-51e9-5a7b-114e99ab6370"
sessionid=42445 proto=6 action="server-rst" user="Jack" group="QA" policyid=1
policytype="consolidated" centralnatid=1 service="HTTPS" dstcountry="United States"
srccountry="Reserved" trandisp="snat" transip=172.16.200.2 transport=56572 duration=6
sentbyte=276 rcvdbyte=745 sentpkt=5 rcvdpkt=11 appid=15832 app="Facebook"
appcat="Social.Media" apprisk="medium" utmaction="allow" countapp=1 utmref=65531-294
```

```
2: date=2019-06-17 time=16:47:45 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="vd1" eventtime=1560815265058557636 tz="-0700" srcip=10.1.100.102
srcport=56668 srcintf="port18" srcintfrole="undefined" dstip=172.217.3.165 dstport=443
dstintf="port17" dstintfrole="undefined" poluid="b740d418-8ed3-51e9-5a7b-114e99ab6370"
sessionid=43201 proto=6 action="timeout" user="Jack" group="QA" policyid=1
policytype="consolidated" centralnatid=1 service="HTTPS" dstcountry="United States"
srccountry="Reserved" trandisp="snat" transip=172.16.200.2 transport=56668 duration=303
sentbyte=406 rcvdbyte=384 sentpkt=4 rcvdpkt=4 appcat="unscanned" utmaction="allow"
countweb=1 utmref=65531-3486
```

## Other NGFW policy-based mode options

You can combine *Application Control* and *Web Filter* in the same NGFW mode policy. If the policy accepts applications or URL categories, you can also apply *AntiVirus*, *DNS Filter*, *IPS* profiles, and logging options.

## NGFW policy mode application default service

In NGFW policy-based mode, the application default service enforces applications running only on their default service port. The applications specified in the policy are monitored, and if traffic is detected from a nonstandard port, it is blocked, and a log entry is recorded with a *port-violation* event type.

If you are not using the default ports, and need to pick specific services, select *Specify* to select the required services.

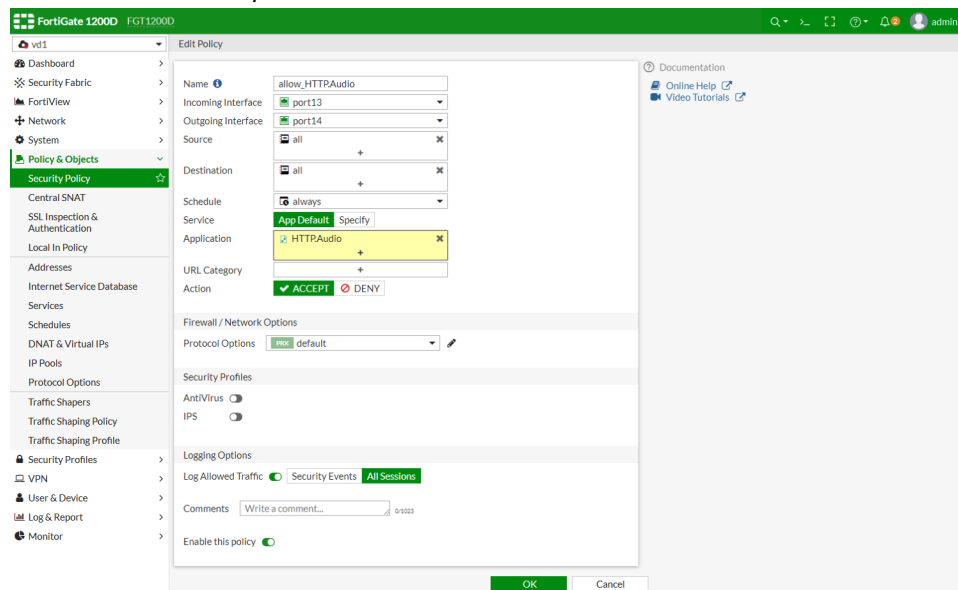
## Example

In this example, the standard port is enforced for HTTPS traffic using the HTTP.Audio application.

First, an SSL Inspection & Authentication policy is created do to traffic pre-match, and then a security policy is created to allow the HTTP.Audio application when using the default port. Fetching an MP3 file from an HTTP server using port 443 is allowed, but is blocked when using a nonstandard port, such as 8443.

### To enforce the HTTP.Audio application using the default port in the GUI:

1. Create a new SSL Inspection & Authentication policy, or use the default policy.
2. Go to *Policy & Objects > Security Policy*, and click *Create New*.
3. Enter a name for the policy, such as *allow\_HTTP.Audio*.
4. Configure the ports as needed.
5. Set *Service* to *App Default*.
6. In the *Application* field, select *HTTP.Audio*.
7. Set the *Action* to *Accept*.



8. Click *OK*.

**To enforce the HTTP.Audio application using the default port in the CLI:****1. Create a firewall policy:**

```
config firewall consolidated policy
 edit 1
 set name "consolidated_all"
 set srcintf "port13"
 set dstintf "port14"
 set srcaddr4 "all"
 set dstaddr4 "all"
 set service "ALL"
 set ssl-ssh-profile "new-deep-inspection"
 next
end
```

**2. Create a security policy:**

```
config firewall security-policy
 edit 1
 set name "allow_HTTP.Audio"
 set srcintf "port13"
 set dstintf "port14"
 set srcaddr4 "all"
 set enforce-default-app-port enable
 set action accept
 set schedule "always"
 set logtraffic all
 set application 15879
 next
end
```

**Logs**

The application logs show logs with an event type of `port-violation` for traffic on port 8443 that is blocked, and an event type of `signature` for traffic on port 443 that is allowed.

**Blocked:**

```
2: date=2019-06-18 time=16:15:40 logid="1060028736" type="utm" subtype="app-ctrl"
eventtype="port-violation" level="warning" vd="vd1" eventtime=1560899740218875746 tz="-0700"
appid=15879 srcip=10.1.100.22 dstip=172.16.200.216 srcport=52680 dstport=8443
srcintf="port13" srcintfrole="undefined" dstintf="port14" dstintfrole="undefined" proto=6
service="HTTPS" direction="incoming" policyid=1 sessionid=5041 appcat="Video/Audio"
app="HTTP.Audio" action="block" hostname="172.16.200.216" incidentserialno=1906780850
url="/app_data/story.mp3" securityid=2 msg="Video/Audio: HTTP.Audio," apprisk="elevated"
```

**Allowed:**

```
1: date=2019-06-18 time=16:15:49 logid="1059028704" type="utm" subtype="app-ctrl"
eventtype="signature" level="information" vd="vd1" eventtime=1560899749258579372 tz="-0700"
appid=15879 srcip=10.1.100.22 dstip=172.16.200.216 srcport=54527 dstport=443
srcintf="port13" srcintfrole="undefined" dstintf="port14" dstintfrole="undefined" proto=6
service="HTTPS" direction="incoming" policyid=1 sessionid=5064 appcat="Video/Audio"
app="HTTP.Audio" action="pass" hostname="172.16.200.216" incidentserialno=1139663486
url="/app_data/story.mp3" securityid=2 msg="Video/Audio: HTTP.Audio," apprisk="elevated"
```

## Policy views and policy lookup

This topic provides a sample of firewall policy views and firewall policy lookup.

### Policy views

In *Policy & Objects* policy list page, there are two policy views: *Interface Pair View* and *By Sequence* view.

*Interface Pair View* displays the policies in the order that they are checked for matching traffic, grouped by the pairs of Incoming and Outgoing interfaces. For example, all policies referencing traffic from WAN1 to DMZ are in one section. The policies referencing traffic from DMZ to WAN1 are in another section. The sections are collapsible so that you only need to look at the sections you want.

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Protocol Options	Security Profiles	Log	Bytes
<b>port2 -&gt; port3</b>											
1		all	all	always	ALL	ACCEPT	Enabled	default	UTM		54.11 MB
<b>port2 -&gt; vlan100</b>											
3		all	all	always	ALL	ACCEPT	Enabled	default	UTM		0 B
<b>port3 -&gt; port2</b>											
2		all	all	always	ALL	ACCEPT	Enabled	default	UTM		9.42 kB
<b>vlan100 -&gt; port2</b>											
4		all	all	always	ALL	ACCEPT	Enabled	default	UTM		0 B
<b>Implicit</b>											
0	Implicit Deny	all	all	always	ALL	DENY			Disabled		2.92 kB

*By Sequence* displays policies in the order that they are checked for matching traffic without any grouping.

ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Protocol Options	Security Profiles	Log	Bytes
1		port2	port3	all	all	always	ALL	ACCEPT	Enabled	default	UTM		54.11 MB
2		port3	port2	all	all	always	ALL	ACCEPT	Enabled	default	UTM		9.42 kB
3		port2	vlan100	all	all	always	ALL	ACCEPT	Enabled	default	UTM		0 B
4		vlan100	port2	all	all	always	ALL	ACCEPT	Enabled	default	UTM		0 B
0	Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled		2.92 kB

The default display is *Interface Pair View*. You can switch between the two views except if *any* or multiple-interfaces are applied in the policy.

### How *Any* or multiple-interfaces policy can change the *Interface Pair View*

The FortiGate unit automatically changes the view on the policy list page to *By Sequence* whenever there is a policy containing *any* or multiple-interfaces as the *Source* or *Destination* interface. If the *Interface Pair View* is grayed out, it is likely that one or more policies have used the *any* or multiple-interfaces.

When you use the *any* or multiple-interfaces, the policy goes into multiple sections because it might be any one of a number of interface pairings. Policies are divided into sections using the interface pairings, for example, port1 to port2.

Each section has its own policy order. The order in which a policy is checked for matching criteria to a packet's information is based solely on the position of the policy within its section or within the entire list of policies. If the policy is in multiple sections, FortiGate cannot place the policy in order in multiple sections. Therefore the view can only be *By Sequence*.

ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Protocol Options	Security Profiles	Log	Bytes
1		any	port3	all	all	always	ALL	ACCEPT	Enabled	default		UTM	54.11 MB
2		port3	port2	all	all	always	ALL	ACCEPT	Enabled	default		UTM	9.42 kB
3		port2	vlan100	all	all	always	ALL	ACCEPT	Enabled	default		UTM	0 B
4		vlan100	port2	all	all	always	ALL	ACCEPT	Enabled	default		UTM	0 B
0	Implicit Deny	any	any	all	all	always	ALL	DENY				Disabled	2.92 kB

## Policy lookup

Firewall policy lookup is based on the `Source_interfaces/Protocol/Source_Address/Destination_Address` that matches the `source-port` and `dst-port` of the protocol. Use this tool to find out which policy matches specific traffic from a number of policies. After completing the lookup, the matching firewall policy is highlighted on the policy list page.

The Policy Lookup tool has the following requirements:

- Transparent mode does not support Policy lookup function.
- When executing the policy lookup, you need to confirm whether the relevant route required for the policy work already exists.

## Sample configuration

This example uses the TCP protocol to show how policy lookup works:

1. In *Policy & Objects* policy list page, click *Policy Lookup* and enter the traffic parameters.

Policy Lookup

Source Interface: port2

Protocol: TCP

Source: 10.1.100.11

Source Port: 12345

Destination: 172.16.200.55

Destination Port: 80

Search Cancel

2. Click *Search* to display the policy lookup results.

ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Protocol Options	Security Profiles	Log	Bytes
1		port2	port3	10-1-100-0	172-16-200-0	always	ALL	ACCEPT	Enabled	default		UTM	54.11 MB
2		port3	port2	all	all	always	ALL	ACCEPT	Enabled	default		UTM	9.42 kB
3		port2	vlan100	all	all	always	ALL	ACCEPT	Enabled	default		UTM	0 B
4		vlan100	port2	all	all	always	ALL	ACCEPT	Enabled	default		UTM	0 B
0	Implicit Deny	any	any	all	all	always	ALL	DENY				Disabled	2.92 kB

## Policy with source NAT

The following recipes provide instructions on configuring policies with source NAT:

- [Static SNAT on page 777](#)
- [Dynamic SNAT on page 778](#)
- [Central SNAT on page 783](#)

## Static SNAT

Network Address Translation (NAT) is the process that enables a single device such as a router or firewall to act as an agent between the Internet or Public Network and a local or private network. This agent acts in real time to translate the source or destination IP address of a client or server on the network interface. For the source IP translation, this enables a single public address to represent a significantly larger number of private addresses. For the destination IP translation, the firewall can translate a public destination address to a private address. So we don't have to configure a real public IP address for the server deployed in a private network.

We can subdivide NAT into two types: source NAT (SNAT) and destination NAT (DNAT). This topic is about SNAT, We support three NAT working modes: static SNAT, dynamic SNAT, and central SNAT.

In static SNAT all internal IP addresses are always mapped to the same public IP address. This is a port address translation, Since we have 60416 available port numbers, this one public IP address can handle the conversion of 60,416 internal IP addresses. See example below.

Internal Source IP	Source Port	Translated Source IP	Translated Source Port
10.1.100.1	11110	172.16.200.1	5117
10.1.100.1	11111	172.16.200.1	5118
10.1.100.2	11112	172.16.200.1	5119
*****	*****	172.16.200.1	*****
*****	*****	172.16.200.1	65533

FortiGate firewall configurations commonly use the Outgoing Interface address.

## Sample configuration

The following example of static SNAT uses an internal network with subnet 10.1.100.0/24 (vlan20) and an external/ISP network with subnet 172.16.200.0/24 (vlan30).

When the clients in internal network need to access the servers in external network, We need to translate IP addresses from 10.1.100.0/24 to an IP address 172.16.200.0/24, In this example, we implement static SNAT by creating a firewall policy.

### To configure static NAT:

1. In *Policy & Objects > IPv4 Policy*, click *Create New*.
2. Enter the required policy parameters.
3. Enable *NAT* and select *Use Outgoing Interface Address*.
4. If needed, enable *Preserve Source Port*.  
 Enable *Preserve Source Port* to keep the same source port for services that expect traffic to come from a specific source port.  
 Disable *Preserve Source Port* to allow more than one connection through the firewall for that service.

Name			
Incoming Interface	To_vlan20 (wan2)	✕	
	+		
Outgoing Interface	To_vlan30 (wan1)	✕	
	+		
Source	10-1-100-0	✕	
	+		
Destination	172-16-200-0	✕	
	+		
Schedule	always	▼	
Service	ALL	✕	
	+		
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN <input type="checkbox"/> IPsec		
Firewall / Network Options			
NAT	<input checked="" type="checkbox"/>		
IP Pool Configuration	<input checked="" type="checkbox"/> Use Outgoing Interface Address <input type="checkbox"/> Use Dynamic IP Pool		
Preserve Source Port	<input type="checkbox"/>		
Protocol Options	<input checked="" type="checkbox"/> PRX default <input type="checkbox"/>		

For packets that match this policy, its source IP address is translated to the IP address of the outgoing interface.

## Dynamic SNAT

Dynamic SNAT maps the private IP addresses to the first available public address from a pool of addresses. In the FortiGate firewall, this can be done by using IP pools. IP pools is a mechanism that allows sessions leaving the FortiGate firewall to use NAT. An IP pool defines a single IP address or a range of IP addresses to be used as the source address for the duration of the session. These assigned addresses are used instead of the IP address assigned to that FortiGate interface.

### IP pool types

FortiGate uses four types of IPv4 IP pools. This recipe focuses on some of the differences between them.

#### Overload

This type of IP pool is similar to static SNAT mode. We need to define an external IP range that contains one or more IP addresses. When there is only one IP address it is almost the same as static SNAT, the outgoing interface address is used. When it contains multiple IP addresses, it is equivalent to an extended mode of static SNAT.

For instance, if we define an overload type IP pool with two external IP addresses (172.16.200.1—172.16.200.2), since there are 60,416 available port numbers per IP, this IP pool can handle 60,416\*2 internal IP addresses.

Original Source IP	Original Source Port	Translated Source IP	Translated Source Port
10.1.100.1	11110	172.16.200.1	5117
10.1.100.2	11111	172.16.200.1	5118
*****	*****	172.16.200.1	*****
*****	*****	172.16.200.1	65533
*****	*****	172.16.200.2	5117
*****	*****	*****	*****
*****	*****	172.16.200.2	65533

The mapped IP address can be calculated from the source IP address. The index number of the address in the pool is the remainder of the source IP address, in decimal, divided by the number addresses in the pool.





To calculate the decimal value of the source IP address, either use an online calculator, or use the following equation:

$$a.b.c.d = a * (256)^3 + b * (256)^2 + c * (256) + d$$

For example:

$$192.168.0.1 = 192 * (256)^3 + 168 * (256)^2 + 0 * (256) + 1 = 3232235521$$

If there is one IP pool, where:

- $P_1$  = the first address in the IP pool
- $R_1$  = the number of IP addresses in the IP pool
- $X$  = the source IP address as a decimal number
- $Y$  = the mapped IP address

Then the equation to determine the mapped address is:

$$Y = P_1 + X \bmod R_1$$

For example:

IP pool	Source IP address
172.26.73.20 to 172.26.73.90	192.168.1.200

1. Convert the source IP address to a decimal number:

$$192 * (256)^3 + 168 * (256)^2 + 1 * (256) + 200 = 3232235976$$

2. Determine the number of IP addresses in the pool:

$$172.26.73.90 - 172.26.73.20 = 71$$

3. Find the remainder of the source IP address divided by the number of addresses in the pool:

$$3232235976 \bmod 71 = 26$$

4. Add the remainder to the first IP address in the pool:

$$172.26.73.20 + 26 = 172.26.73.46$$

So, the mapped IP address is **172.26.73.46**.

If there are multiple IP pools, the calculation is similar to when there is only one pool.

If there are two IP pools, where:

- $P_1$  = the first address in the first IP pool
- $P_2$  = the first address in the second IP pool
- $R_1$  = the number of IP addresses in the first IP pool
- $R_2$  = the number of IP addresses in the second IP pool
- $X$  = the source IP address as a decimal number
- $Y$  = the mapped IP address

Then the equations to determine the mapped address are:

$$\text{If } X \bmod (R_1 + R_2) \geq R_1, \text{ then } Y = P_2 + X \bmod R_2$$

$$\text{If } X \bmod (R_1 + R_2) < R_1, \text{ then } Y = P_1 + X \bmod R_1$$

For example:

IP pools	Source IP address
pool01: 172.26.73.20 to 172.26.73.90	192.168.1.200
pool02: 172.26.75.50 to 172.26.75.150	

1. Convert the source IP address to a decimal number:

$$192 * (256)^3 + 168 * (256)^2 + 1 * (256) + 200 = 3232235976$$

2. Determine the total number of IP addresses in the pools:

$$(172.26.73.90 - 172.26.73.20) + (172.26.75.50 - 172.26.75.150) = 71 + 101 = 172$$

3. Find the remainder of the source IP address divided by the number of addresses in the pools:

$$3232235976 \text{ mod } 172 = 108$$

4. The remainder is greater than the number of addresses in pool01, so the address is selected from pool02 and the remainder is recalculated based only on pool02:

$$3232235976 \text{ mod } 101 = 40$$

5. Add the new remainder to the first IP address in pool02:

$$172.26.75.50 + 40 = 172.26.75.90$$

So, the mapped IP address is **172.26.75.90**.

### One-to-one

This type of IP pool means that the internal IP address and the external (translated) IP address match one-to-one. The port address translation (PAT) is disabled when using this type of IP pool. For example, if we define a one-to-one type IP pool with two external IP addresses (172.16.200.1 - 172.16.200.2), this IP pool only can handle two internal IP addresses.

### Fixed port range

For the overload and one-to-one IP pool types, we do not need to define the internal IP range. For the fixed port range type of IP pool, we can define both internal IP range and external IP range. Since each external IP address and the number of available port numbers is a specific number, if the number of internal IP addresses is also determined, we can calculate the port range for each address translation combination. So we call this type fixed port range. This type of IP pool is a type of port address translation (PAT).

For instance, if we define one external IP address (172.16.200.1) and ten internal IP addresses (10.1.100.1-10.1.100.10), we have translation IP+Port combination like following table:

Original Source IP	Original Source Port	Translated Source IP	Translated Source Port Range
10.1.100.1	*****	172.16.200.1	5117~11157
10.1.100.2	*****	172.16.200.1	11158~17198
10.1.100.3	*****	172.16.200.1	*****
10.1.100.4	*****	172.16.200.1	*****
10.1.100.5	*****	172.16.200.1	*****
10.1.100.6	*****	172.16.200.1	*****
10.1.100.7	*****	172.16.200.1	*****
10.1.100.8	*****	172.16.200.1	*****
10.1.100.9	*****	172.16.200.1	53445~59485
10.1.100.10	*****	172.16.200.1	59486~65526

## Port block allocation

This type of IP pool is also a type of port address translation (PAT). It gives users a more flexible way to control the way external IPs and ports are allocated. Users need to define *Block Size/Block Per User* and external IP range. *Block Size* means how many ports each Block contains. *Block per User* means how many blocks each user (internal IP) can use.

The following is a simple example:

- **External IP Range:** 172.16.200.1—172.16.200.1
- **Block Size:** 128
- **Block Per User:** 8

Result:

- **Total-PBAs:** 472 (60416/128)
- **Maximum ports can be used per User (Internal IP Address):** 1024 (128\*8)
- **How many Internal IP can be handled:** 59 (60416/1024 or 472/8)

## Sample configuration

To configure overload IP pool in the GUI:

1. In *Policy & Objects > IP Pools*, click *Create New*.
2. Select *IPv4 Pool* and then select *Overload*.

The screenshot shows the 'New Dynamic IP Pool' configuration window. The 'IP Pool Type' is set to 'IPv4 Pool'. The 'Name' is 'Overload-ippool'. The 'Comments' field is empty with a character count of 0/255. The 'Type' is set to 'Overload'. The 'External IP Range' is '172.16.200.1 - 172.16.200.1'. The 'ARP Reply' checkbox is checked. At the bottom, there are 'OK' and 'Cancel' buttons.

To configure overload IP pool in the CLI:

```
config firewall ippool
 edit "Overload-ippool"
 set startip 172.16.200.1
 set endip 172.16.200.1
 next
end
```

### To configure one-to-one IP pool using the GUI:

1. In *Policy & Objects > IP Pools*, click *Create New*.
2. Select *IPv4 Pool* and then select *One-to-One*.

New Dynamic IP Pool

IP Pool Type: **IPv4 Pool** | IPv6 Pool

Name: One-to-One-ippool

Comments: 0/255

Type: Overload | **One-to-One** | Fixed Port Range | Port Block Allocation

External IP Range: 172.16.200.1 - 172.16.200.2

ARP Reply: ☒

OK Cancel

### To configure one-to-one IP pool in the CLI:

```
config firewall ippool
 edit "One-to-One-ippool"
 set type one-to-one
 set startip 172.16.200.1
 set endip 172.16.200.2
 next
end
```

### To configure fixed port range IP pool in the GUI:

1. In *Policy & Objects > IP Pools*, click *Create New*.
2. Select *IPv4 Pool* and then select *Fixed Port Range*.

New Dynamic IP Pool

IP Pool Type: **IPv4 Pool** | IPv6 Pool

Name: FPR-ippool

Comments: 0/255

Type: Overload | One-to-One | **Fixed Port Range** | Port Block Allocation

External IP Range: 172.16.200.1 - 172.16.200.1

Internal IP Range: 10.1.100.1 - 10.1.100.10

ARP Reply: ☒

OK Cancel

### To configure fixed port range IP pool in the CLI:

```
config firewall ippool
 edit "FPR-ippool"
 set type fixed-port-range
 set startip 172.16.200.1
 set endip 172.16.200.1
 set source-startip 10.1.100.1
 set source-endip 10.1.100.10
 next
end
```

### To configure port block allocation IP pool in the GUI:

1. In *Policy & Objects > IP Pools*, click *Create New*.
2. Select *IPv4 Pool* and then select *Port Block Allocation*.

New Dynamic IP Pool

IP Pool Type: **IPv4 Pool** | IPv6 Pool

Name: PBA-ippool

Comments: 0/255

Type: Overload | One-to-One | Fixed Port Range | **Port Block Allocation**

External IP Range: 172.16.200.1 - 172.16.200.1

Block Size: 128

Blocks Per User: 8

ARP Reply: ☒

OK Cancel

### To configure port block allocation IP pool in the CLI:

```
config firewall ippool
 edit PBA-ippool
 set type port-block-allocation
 set startip 172.16.200.1
 set endip 172.16.200.1
 set block-size 128
 set num-blocks-per-user 8
 next
end
```

## Central SNAT

The central SNAT table enables you to define and control (with more granularity) the address translation performed by FortiGate. With the NAT table, you can define the rules for the source address or address group, and which IP pool the destination address uses.

While similar in functionality to IP pools where a single address is translated to an alternate address from a range of IP addresses, with IP pools there is no control over the translated port. When using the IP pool for source NAT, you can define a fixed port to ensure the source port number is unchanged. If no fixed port is defined, the port translation is randomly chosen by FortiGate. With the central NAT table, you have full control over both the IP address and port translation.

FortiGate reads the NAT rules from the top down until it hits a matching rule for the incoming address. This enables you to create multiple NAT policies that dictate which IP pool is used based on the source address. NAT policies can be rearranged within the policy list. NAT policies are applied to network traffic after a security policy.

The central SNAT table allows you to create, edit, delete, and clone central SNAT entries.

### Central SNAT notes

- The central NAT feature is not enabled by default.
- If central NAT is enabled, the NAT option under IPv4 policies is skipped and SNAT must be done via `central-snat-map`. The IPv4 policy list and dialog boxes have messages and redirection links to show this information.
- If NGFW mode is policy-based, then it is assumed that central NAT (specifically SNAT) is enabled implicitly.

- The option to toggle NAT in `central-snat-map` policies has been added. Previously it was only shown in NGFW policy-based mode.
- In the central SNAT policy dialog box, the port mapping fields for the original port have been updated to accept ranges.
- If per VDOM NAT is enabled, NAT is skipped in firewall policy.
- The central SNAT window contains a table of all the central SNAT policies.

## Sample configuration

### To enable or disable central SNAT using the CLI:

```
config system settings
 set central-nat [enable | disable]
end
```

When central NAT is enabled, *Policy & Objects* displays the Central SNAT section.

### To create central SNAT using the GUI:

1. In *Policy & Objects > Central SNAT*.  
The right pane displays a table of Central SNAT entries.
2. To create a new entry, click *Create New* in the right pane.  
To edit an entry, double-click the policy you want to edit.
3. To set the *Incoming Interface*, click + in that field.
4. In the pane on the right, select an interface to add it.  
You can select multiple interfaces.
5. To set the *Outgoing Interface*, click click + in that field.
6. In the pane on the right, select an interface to add it.  
You can select multiple interfaces.
7. To set the *Source Address*, click click + in that field.
8. In the pane on the right, select an address to add it.  
You can select multiple addresses.
9. To set the *Destination Address*, click click + in that field.
10. In the pane on the right, select an address to add it.  
You can select multiple addresses.
11. In *NAT > IP Pool Configuration*, select either *Use Outgoing Interface Address* or *Use Dynamic IP Pool*.  
If you select *Use Dynamic IP Pool*, click + and select which IP pool to use.
12. Select one of the following *Protocol* parameters.
  - *ANY*. Use any protocol traffic.
  - *TCP*. Use TCP traffic only. Protocol number is set to 6.
  - *UDP*. Use UDP traffic only. Protocol number is set to 17.
  - *SCTP*. Use SCTP traffic only. Protocol number is set to 132.
  - *Specify*. You can specify the traffic filter protocol by setting the protocol number.
13. If you use the *Overload* type of IP pool, you can enable *Explicit Port Mapping*.
  - a. If you enable *Explicit Port Mapping*, set the *Original Source Port* to the start number of the source port range.
  - b. Set the *Translated Port* to the start number of the translated port range.
14. Click *OK*.

**To configure central SNAT using the CLI:**

```
config firewall central-snat-map
edit <policyID number>set status [enable|disable]
 set orig-addr <valid address object preconfigured on the FortiGate>
 set srcintf <name of interface on the FortiGate>
 set dst-addr <valid address object preconfigured on the FortiGate>
 set dstintf <name of interface on the FortiGate>
 set protocol <integer for protocol number>
 set orig-port <integer for original port number>
 set nat-port <integer for translated port number>
 set comments <string>
end
```

**To set NAT to be not available regardless of NGFW mode:**

```
config firewall central-snat-map
 edit 1
 set orig-addr "192-86-1-86"
 set srcintf "port23"
 set dst-addr "192-96-1-96"
 set dstintf "port22"
 set nat-ippool "pool1"
 set protocol 17
 set orig-port 2896-2897
 set nat enable
 next
end
```

**To hide NAT port if NAT IP pool is not set or if NAT is disabled:**

```
config firewall central-snat-map
 edit 1
 set orig-addr "192-86-1-86"
 set srcintf "port23"
 set dst-addr "192-96-1-96"
 set dstintf "port22"
 set nat-ippool "pool1"
 set protocol 17
 set orig-port 2896-2897
 set nat disable
 next
end
```

**To change original port to accept range:**

```
config firewall central-snat-map
 edit 1
 set orig-addr "192-86-1-86"
 set srcintf "port23"
 set dst-addr "192-96-1-96"
 set dstintf "port22"
 set nat-ippool "pool1"
 set protocol 17
 set orig-port 2896-2897 (help text changed to: Original port or port range).
```

```
 set nat-port 35804-35805
 next
end
```

## Policy with destination NAT

The following recipes provide instructions on configuring policies with destination NAT:

- [Static virtual IPs on page 786](#)
- [Virtual IP with services on page 787](#)
- [Virtual IPs with port forwarding on page 789](#)
- [Virtual server on page 791](#)

### Static virtual IPs

Mapping a specific IP address to another specific IP address is usually called Destination NAT (DNAT). When this central NAT table is not used, FortiOS calls this a Virtual IP address (VIP). DNAT, or VIP, is used to map an external IP address to an IP address or address range. The mapping can include all TCP/UDP ports or, if port forwarding is enabled, it only refers to the specific configured ports. As the central NAT table is disabled by default, the term VIP is usually used.

VIPs are typically used to NAT external or public IP addresses to internal or private IP addresses. Using a VIP between two internal interfaces made up of private IP addresses is possible, but rare, because the two networks can just use the IP addresses of the networks without any address translation. Using a VIP for traffic going from the inside to the internet is supported, but unlikely to be required.

### Sample configuration

**To create a virtual IP using the GUI:**

1. In *Policy & Objects > Virtual IPs*.
2. Click *Create New* and select *Virtual IP*.
3. Select a *VIP Type* based on the IP versions used:
  - If IPv4 is on both sides of the FortiGate unit, select *IPv4*.
  - If IPv6 is on both sides of the FortiGate unit, select *IPv6*.
  - If traffic goes from an IPv4 network to an IPv6 network, select *NAT46*.
  - If traffic goes from an IPv6 network to an IPv4 network, select *NAT64*.



#### 4. Enter a unique name for the virtual IP and fill in the other fields.

#### To create a virtual IP using the CLI:

```
config firewall vip
 edit "Internal_WebServer"
 set extip 10.1.100.199
 set extintf "any"
 set mappedip "172.16.200.55"
 next
end
```

#### To apply a virtual IP to policy using the CLI:

```
config firewall policy
 edit 8
 set name "Example_Virtual_IP_in_Policy"
 set srcintf "wan2"
 set dstintf "wan1"
 set srcaddr "all"
 set dstaddr "Internal_WebServer"
 set action accept
 set schedule "always"
 set service "ALL"
 set nat enable
 next
end
```

## Virtual IP with services

Virtual IP with services is a more flexible virtual IP mode. This mode allows users to define services to a single port number mapping.

This recipe shows how to use virtual IP with services enabled. This example has one public external IP address. We map TCP ports 8080, 8081, and 8082 to an internal WebServer TCP port 80. This allows remote connections to communicate with a server behind the firewall.

## Sample configuration

### To create a virtual IP with services using the GUI:

1. In *Policy & Objects > Virtual IPs*.
2. Click *Create New* and select *Virtual IP*.
3. For *VIP Type*, select *IPv4*.
4. Enter a unique name for the virtual IP and fill in the other fields.
5. Configure the fields in the *Network* section. For example:
  - Set *Interface* to *any*.
  - Set *External IP Address/Range* to *10.1.100.199*.
  - Set *Mapped IP Address/Range* to *172.16.200.55*.
6. Enable *Optional Filters* and then enable *Services*.
7. In the *Services* field, click + to display the Services pane.
8. In the *Services* pane, select *TCP\_8080*, *TCP\_8081*, and *TCP\_8082*.
9. Enable *Port Forwarding*.
10. Set *Map to Port* to *80*.

11. Click *OK*.

### To see the results:

1. Apply the above virtual IP to the Firewall policy.
2. The results are:
  - Access 10.1.100.199:8080 from external network and FortiGate maps to 172.16.200.55:80 in internal network.
  - Access 10.1.100.199:8081 from external network and FortiGate maps to 172.16.200.55:80 in internal network.
  - Access 10.1.100.199:8082 from external network and FortiGate maps to 172.16.200.55:80 in internal network.

**To create a virtual IP with services using the CLI:**

```
config firewall vip
 edit "WebServer_VIP_Services"
 set service "TCP_8080" "TCP_8081" "TCP_8082"
 set extip 10.1.100.199
 set extintf "any"
 set portforward enable
 set mappedip "172.16.200.55"
 set mappedport 80
 next
end
```

## Virtual IPs with port forwarding

If you need to hide the internal server port number or need to map several internal servers to the same public IP address, enable port-forwarding for Virtual IP.

This recipe shows how to use virtual IPs to configure port forwarding on a FortiGate unit. This example has one public external IP address. We map TCP ports 8080, 8081, and 8082 to different internal WebServers' TCP port 80. This allows remote connections to communicate with a server behind the firewall.

## Sample configuration

**To create a virtual IP with port forwarding using the GUI:**

1. In *Policy & Objects > Virtual IPs*.
2. Click *Create New* and select *Virtual IP*.
3. For *VIP Type*, select *IPv4*.
4. Enter a unique name for the virtual IP and fill in the other fields.
5. Configure the fields in the *Network* section. For example:
  - Set *Interface* to *any*.
  - Set *External IP Address/Range* to *10.1.100.199*.
  - Set *Mapped IP Address/Range* to *172.16.200.55*.
6. Leave *Optional Filters* disabled.
7. Enable *Port Forwarding*.
8. Configure the fields in the *Port Forwarding* section. For example:
  - Set *Protocol* to *TCP*.
  - Set *External Service Port* to *8080 - 8080*.
  - Set *Map to Port* to *80 - 80*.

**Edit Virtual IP**

VIP Type: IPv4

Name: WebServer\_8080

Comments:

Color: Change

---

**Network**

Interface:

Type: Static NAT

External IP Address/Range: 10.1.100.199 - 10.1.100.199

Mapped IP Address/Range: 172.16.200.55 - 172.16.200.55

---

Optional Filters: ☐

---

Port Forwarding: ☒

Protocol: ☒ TCP ☐ UDP ☐ SCTP ☐ ICMP

External Service Port: 8080 - 8080

Map to Port: 80 - 80

OK Cancel

9. Click **OK**.
10. Follow the above steps to create two additional virtual IPs.
  - a. For one virtual IP:
    - Use a different *Mapped IP Address/Range*, for example, 172.16.200.56.
    - Set *External Service Port* to 8081 - 8081.
    - Use the same *Map to Port* numbers: 80 - 80.
  - b. For the other virtual IP:
    - Use a different *Mapped IP Address/Range*, for example, 172.16.200.57.
    - Set *External Service Port* to 8082 - 8082.
    - Use the same *Map to Port* numbers: 80 - 80.
11. Create a *Virtual IP Group* and put the above three virtual IPs into that group.

**Edit VIP Group**

Type: ☒ IPv4 ☐ IPv6 ☐ NAT46 ☐ NAT64

Name: WebServer\_VIP

Comments:

Color: Change

Interface:

Members:

WebServer_8080	✕
WebServer_8081	✕
WebServer_8082	✕
+	

OK Cancel

### To see the results:

1. Apply the above virtual IP to the Firewall policy.
2. The results are:
  - Access 10.1.100.199:8080 from external network and FortiGate maps to 172.16.200.55:80 in internal network.
  - Access 10.1.100.199:8081 from external network and FortiGate maps to 172.16.200.56:80 in internal network.
  - Access 10.1.100.199:8082 from external network and FortiGate maps to 172.16.200.57:80 in internal network

## Virtual server

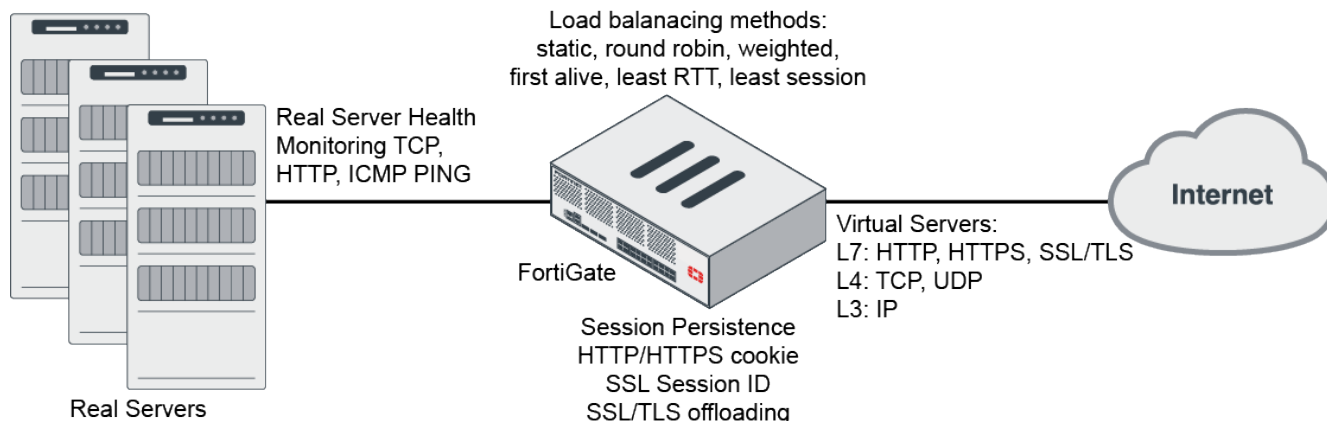
This topic shows a special virtual IP type: virtual server. Use this type of VIP to implement server load balancing.

The FortiOS server load balancing contains all the features of a server load balancing solution. You can balance traffic across multiple backend servers based on multiple load balancing schedules including:

- Static (failover)
- Round robin
- Weighted (to account for different sized servers or based on the health and performance of the server including round trip time and number of connections)

The load balancer supports HTTP, HTTPS, IMAPS, POP3S, SMTPS, SSL/TLS, and generic TCP/UDP and IP protocols. Session persistence is supported based on the SSL session ID based on an injected HTTP cookie, or based on the HTTP or HTTPS host. SSL/TLS load balancing includes protection from protocol downgrade attacks. Server load balancing is supported on most FortiGate devices and includes up to 10,000 virtual servers on high end systems.

## Sample topology



## SSL/TLS offloading

FortiGate SSL/TLS offloading is designed for the proliferation of SSL/TLS applications. The key exchange and encryption/decryption tasks are offloaded to the FortiGate unit where they are accelerated using FortiASIC technology which provides significantly more performance than a standard server or load balancer. This frees up valuable resources on the server farm to give better response to business operations. Server load balancing offloads most SSL/TLS versions including SSL 3.0, TLS 1.0, and TLS 1.2, and supports full mode or half mode SSL offloading with DH key sizes up to 4096 bits.

FortiGate SSL offloading allows the application payload to be inspected before it reaches your servers. This prevents intrusion attempts, blocks viruses, stops unwanted applications, and prevents data leakage. SSL/TLS content inspection supports TLS versions 1.0, 1.1, and 1.2 and SSL versions 1.0, 1.1, 1.2, and 3.0.

## Virtual server requirements

When creating a new virtual server, you must configure the following options:

- Virtual Server Type.
- Load Balancing Methods.

- Health check monitoring (optional).
- Session persistence (optional).
- Virtual Server IP (External IP Address).
- Virtual Server Port (External Port).
- Real Servers (Mapped IP Address & Port).

### Virtual server types

Select the protocol to be load balanced by the virtual server. If you select a general protocol such as IP, TCP, or UDP, the virtual server load balances all IP, TCP, or UDP sessions. If you select specific protocols such as HTTP, HTTPS, or SSL, you can apply additional server load balancing features such as *Persistence* and *HTTP Multiplexing*.

<b>HTTP</b>	Select <i>HTTP</i> to load balance only HTTP sessions with the destination port number that matches the <i>Virtual Server Port</i> setting. Change <i>Virtual Server Port</i> to match the destination port of the sessions to be load balanced (usually port 80 for HTTP sessions). You can enable <i>HTTP Multiplexing</i> . You can also set <i>Persistence</i> to <i>HTTP Cookie</i> to enable cookie-based persistence.
<b>HTTPS</b>	Select <i>HTTPS</i> to load balance only HTTPS sessions with the destination port number that matches the <i>Virtual Server Port</i> setting. Change <i>Virtual Server Port</i> to match the destination port of the sessions to be load balanced (usually port 443 for HTTPS sessions). You can enable <i>HTTP Multiplexing</i> . You can also set <i>Persistence</i> to <i>HTTP Cookie</i> to enable cookie-based persistence, or you can set <i>Persistence</i> to <i>SSL Session ID</i> .
<b>IMAPS</b>	Select <i>IMAPS</i> to load balance only IMAPS sessions with the destination port number that matches the <i>Virtual Server Port</i> setting. Change <i>Virtual Server Port</i> to match the destination port of the sessions to be load balanced (usually port 993 for IMAPS sessions). You can also set <i>Persistence</i> to <i>SSL Session ID</i> .
<b>POP3S</b>	Select <i>POP3S</i> to load balance only POP3S sessions with the destination port number that matches the <i>Virtual Server Port</i> setting. Change <i>Virtual Server Port</i> to match the destination port of the sessions to be load balanced (usually port 995 for POP3S sessions). You can also set <i>Persistence</i> to <i>SSL Session ID</i> .
<b>SMTPS</b>	Select <i>SMTPS</i> to load balance only SMTPS sessions with the destination port number that matches the <i>Virtual Server Port</i> setting. Change <i>Virtual Server Port</i> to match the destination port of the sessions to be load balanced (usually port 465 for SMTPS sessions). You can also set <i>Persistence</i> to <i>SSL Session ID</i> .
<b>SSL</b>	Select <i>SSL</i> to load balance only SSL sessions with the destination port number that matches the <i>Virtual Server Port</i> setting. Change <i>Virtual Server Port</i> to match the destination port of the sessions to be load balanced. You can also set <i>Persistence</i> to <i>SSL Session ID</i> .
<b>TCP</b>	Select <i>TCP</i> to load balance only TCP sessions with the destination port number that matches the <i>Virtual Server Port</i> setting. Change <i>Virtual Server Port</i> to match the destination port of the sessions to be load balanced.
<b>UDP</b>	Select <i>UDP</i> to load balance only UDP sessions with the destination port number that matches the <i>Virtual Server Port</i> setting. Change <i>Virtual Server Port</i> to match the destination port of the sessions to be load balanced.
<b>IP</b>	Select <i>IP</i> to load balance all sessions accepted by the security policy that contains this virtual server.

## Load balancing methods

The load balancing method defines how sessions are load balanced to real servers.

All load balancing methods do not send traffic to real servers that are down or not responding. FortiGate can only determine if a real server is not responding by using a health check monitor. You should always add at least one health check monitor to a virtual server or to real servers; otherwise load balancing might try to distribute sessions to real servers that are not functioning.

<b>Static</b>	The traffic load is statically spread evenly across all real servers. Sessions are not assigned according to how busy individual real servers are. This load balancing method provides some persistence because all sessions from the same source address always go to the same real server. Because the distribution is stateless, so if a real server is added, removed, or goes up or down, the distribution is changed and persistence might be lost.
<b>Round Robin</b>	Directs new requests to the next real server. This method treats all real servers as equals regardless of response time or the number of connections. This method does not direct requests to real servers that down or non responsive.
<b>Weighted</b>	Real servers with a higher weight value receive a larger percentage of connections. Set the real server weight when adding a real server.
<b>Least Session</b>	Directs requests to the real server that has the least number of current connections. This method works best in environments where the real servers or other equipment you are load balancing all have similar capabilities. This load balancing method uses the FortiGate session table to track the number of sessions being processed by each real server. The FortiGate unit cannot detect the number of sessions actually being processed by a real server.
<b>Least RTT</b>	Directs sessions to the real server with the lowest round trip time. The round trip time is determined by a ping health check monitor. The default is 0 if no ping health check monitors are added to the virtual server.
<b>First Alive</b>	Directs sessions to the first live real server. This load balancing schedule provides real server failover protection by sending all sessions to the first live real server. If a real server fails, all sessions are sent to the next live real server. Sessions are not distributed to all real servers so all sessions are processed by the first real server only.
<b>HTTP Host</b>	Load balances HTTP host connections across multiple real servers using the host's HTTP header to guide the connection to the correct real server.

## Health check monitoring

In the FortiGate GUI, you can configure health check monitoring so that the FortiGate unit can verify that real servers are able respond to network connection attempts. If a real server responds to connection attempts, the load balancer continues to send sessions to it. If a real server stops responding to connection attempts, the load balancer assumes that the server is down and does not send sessions to it. The health check monitor configuration determines how the load balancer tests real servers. You can use a single health check monitor for multiple load balancing configurations. You can configure TCP, HTTP, and Ping health check monitors. You usually set the health check monitor to use the same protocol as the traffic being load balanced to it. For example, for an HTTP load balancing configuration, you would normally use an HTTP health check monitor.

## Session persistence

Use persistence to ensure a user is connected to the same real server every time the user makes an HTTP, HTTPS, or SSL request that is part of the same user session. For example, if you are load balancing HTTP and HTTPS sessions to a collection of eCommerce web servers, when users make a purchase, they will be starting multiple sessions as they navigate the eCommerce site. In most cases, all the sessions started by this user during one eCommerce session should be processed by the same real server. Typically, the HTTP protocol keeps track of these related sessions using cookies. HTTP cookie persistence ensure all sessions that are part of the same user session are processed by the same real server.

When you configure persistence, the FortiGate unit load balances a new session to a real server according to the load balance method. If the session has an HTTP cookie or an SSL session ID, the FortiGate unit sends all subsequent sessions with the same HTTP cookie or SSL session ID to the same real server.

## Real servers

Add real servers to a load balancing virtual server to provide information the virtual server requires to send sessions to the server. A real server configuration includes the IP address of the real server and port number the real server receives sessions on. The FortiGate unit sends sessions to the real server's IP address using the destination port number in the real server configuration.

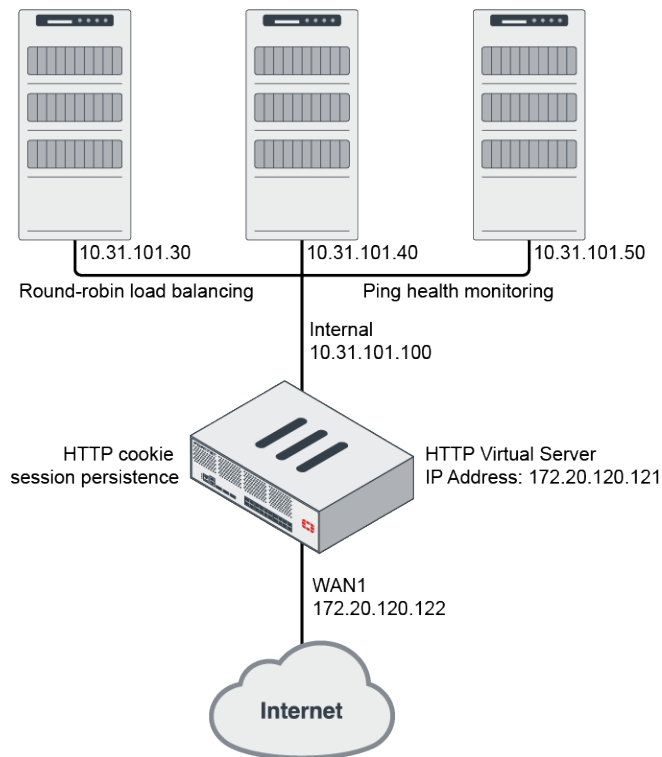
When configuring a real server, you can also specify the weight (if the load balance method is set to *Weighted*) and you can limit the maximum number of open connections between the FortiGate unit and the real server. If the maximum number of connections is reached for the real server, the FortiGate unit automatically switches all further connection requests to other real servers until the connection number drops below the limit. Setting *Maximum Connections* to 0 means that the FortiGate unit does not limit the number of connections to the real server.

## Sample of HTTP load balancing to three real web servers

This example describes the steps to configure the load balancing configuration below. In this configuration, a FortiGate unit is load balancing HTTP traffic from the Internet to three HTTP servers on the internal network. HTTP sessions are accepted at the wan1 interface with destination IP address 172.20.120.121 on TCP port 8080, and forwarded from the internal interface to the web servers. When forwarded, the destination address of the session is translated to the IP address of one of the web servers.

This load balancing configuration also includes session persistence using HTTP cookies, round-robin load balancing, and TCP health monitoring for the real servers. Ping health monitoring consists of the FortiGate unit using ICMP ping to ensure the web servers can respond to network traffic.





### General steps:

1. Create a health check monitor.  
A ping health check monitor causes the FortiGate to ping the real servers every 10 seconds. If one of the servers does not respond within 2 seconds, the FortiGate unit will retry the ping 3 times before assuming that the HTTP server is not responding.
2. Create a load balance virtual server with three real servers.
3. Add the load balancing virtual server to a policy as the destination address.



To see the virtual servers and health check monitors options in the GUI, *Load Balancing* must be selected in *Feature Visibility > Additional Features*. See [Feature visibility on page 732](#) on page 1 for details.

### Configure a load balancing virtual server in the GUI

#### To create a health check monitor:

1. Go to *Policy & Objects > Health Check*.
2. Click *Create New*.
3. Set the following:
  - *Name* to *Ping-mon-1*
  - *Type* to *Ping*
  - *Interval* to *10* seconds
  - *Timeout* to *2* seconds
  - *Retry* to *3* attempt(s)

FortiGate 60E DocsFG

Policy & Objects

New Health Check Monitor

Name: Ping-mon-1

Type: **Ping** TCP HTTP HTTPS

Interval: 10 seconds

Timeout: 2 second(s)

Retry: 3 attempt(s)

OK Cancel

4. Click OK.

### To create a virtual server:

1. Go to *Policy & Objects > Virtual Servers*.
2. Click *Create New*.
3. Set the following:
  - *Name* to *Vserver-HTTP-1*
  - *Type* to *HTTP*
  - *Interface* to *wan1*
  - *Virtual Server IP* to *172.20.120.121*
  - *Virtual Server Port* to *8080*
  - *Load Balance Method* to *Round Robin*
  - *Persistence* to *HTTP Cookie*
  - *Health Check* to *Ping-mon-1*

FortiGate 60E DocsFG

Policy & Objects

New Virtual Server

Type: IPv4

Name: Vserver-HTTP-1

Comments: Write a comment... 0/255

Color: Change

Network

Type: HTTP

Interface: any

Virtual Server IP: 172.20.120.121

Virtual Server Port: 8080

Load Balancing Method: Round Robin

Persistence: None HTTP Cookie

Health Check: Ping-mon-1

HTTP Multiplexing: ☐

Preserve Client IP: ☐

Real Servers

+ Create New Edit Delete

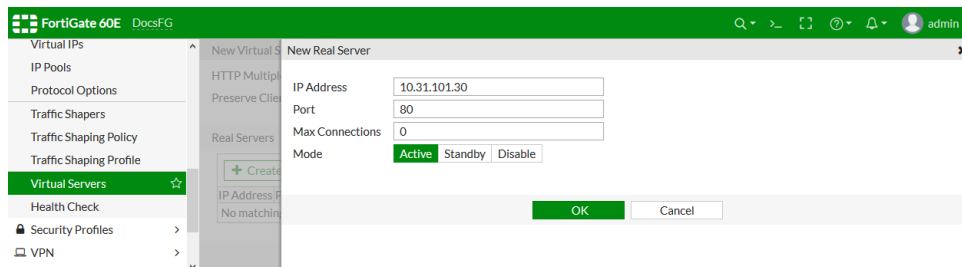
IP Address	Port	Weight	Max Connections	Mode
No matching entries found				

OK Cancel

4. In the *Real Servers* table, click *Create New*.

5. Set the following for the first real server:

- *IP Address* to *10.31.101.30*
- *Port* to *80*
- *Max Connections* to *0*
- *Mode* to *Active*

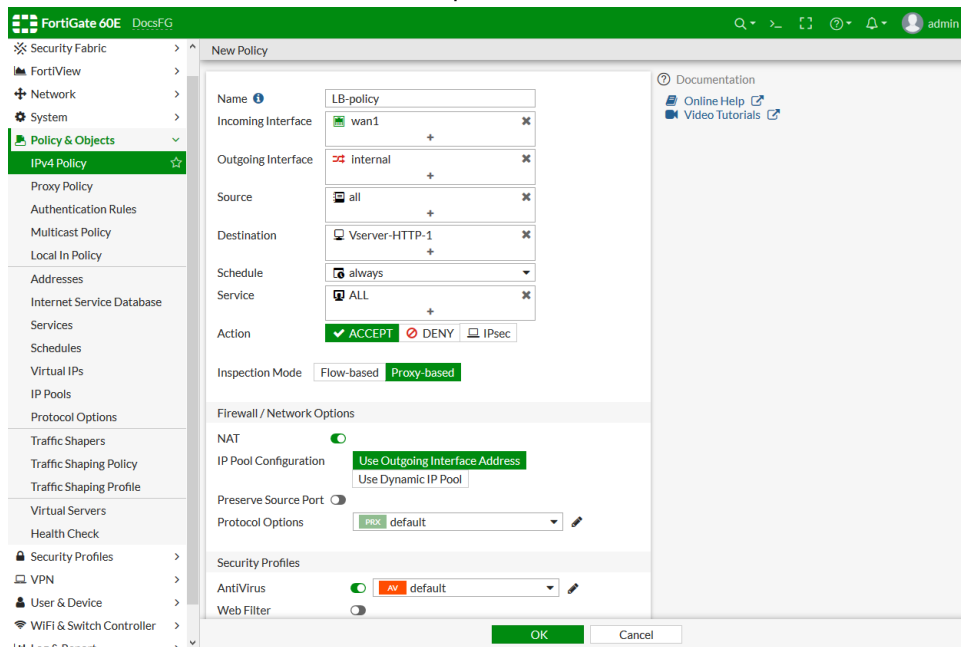


6. Configure two more real servers with IP addresses 10.31.101.40 and 10.31.101.50, and the remaining settings the same as the first real server.
7. Click OK.

**To create a security policy that includes the load balance virtual server as the destination address:**

1. Go to *Policy & Objects > IPv4 Policy*.
2. Click *Create New*.
3. Set the *Inspection Mode* to *Proxy-based*. The new virtual server will not be available if the inspection mode is *Flow-based*.
4. Set the following:
  - *Name* to *LB-policy*
  - *Incoming Interface* to *wan1*
  - *Outgoing Interface* to *internal*
  - *Source* to *all*
  - *Destination* to *Vserver-HTTP-1*
  - *Schedule* to *always*
  - *Service* to *ALL*
  - *Action* to *ACCEPT*
5. Enable NAT and set *IP Pool Configuration* to *Use Outgoing Interface Address*.

## 6. Enable *AntiVirus* and select an antivirus profile.



## 7. Click OK.

## Configure a load balancing virtual server in the CLI

### To configure HTTP load balancing to three real web servers in the CLI:

#### 1. Create a health check monitor:

```
config firewall ldb-monitor
 edit "Ping-mon-1"
 set type ping
 set interval 10
 set timeout 2
 set retry 3
 next
end
```

#### 2. Create a virtual server:

```
config firewall vip
 edit "Vserver-HTTP-1"
 set type server-load-balance
 set extip 172.20.120.121
 set extintf "any"
 set server-type http
 set monitor "Ping-mon-1"
 set ldb-method round-robin
 set persistence http-cookie
 set extport 8080
 config realservers
 edit 1
 set ip 10.31.101.30
 set port 80
 next
 next
 next
end
```

```
 next
 edit 2
 set ip 10.31.101.40
 set port 80
 next
 edit 3
 set ip 10.31.101.50
 set port 80
 next
 end
next
end
```

### 3. Add the load balancing virtual server to a policy as the destination address:

```
config firewall policy
 edit 2
 set name "LB-policy"
 set inspection-mode proxy
 set srcintf "wan1"
 set dstintf "internal"
 set srcaddr "all"
 set dstaddr "Vserver-HTTP-1"
 set action accept
 set schedule "always"
 set service "ALL"
 set utm-status enable
 set ssl-ssh-profile "certificate-inspection"
 set av-profile "default"
 set fsso disable
 set nat enable
 next
end
```

## Results

Traffic accessing 172.20.120.121:8080 is forwarded in turn to the three real servers.

If the access request has an http-cookie, FortiGate forwards the access to the corresponding real server according to the cookie.

## Policy with Internet Service

### Using Internet Service in policy

This recipe shows how to apply a predefined Internet Service entry into a policy.

The Internet Service Database is a comprehensive public IP address database that combines IP address range, IP owner, service port number, and IP security credibility. The data comes from the FortiGuard service system. Information is regularly added to this database, for example, geographic location, IP reputation, popularity & DNS, and so on. All this information helps users define Internet security more effectively. You can use the contents of the database as criteria for inclusion or exclusion in a policy.

From FortiOS version 5.6, Internet Service is included in the firewall policy. It can be applied to a policy only as a destination object. From version 6.0, Internet Service can be applied both as source and destination objects in a policy. You can also apply Internet Services to shaping policy.

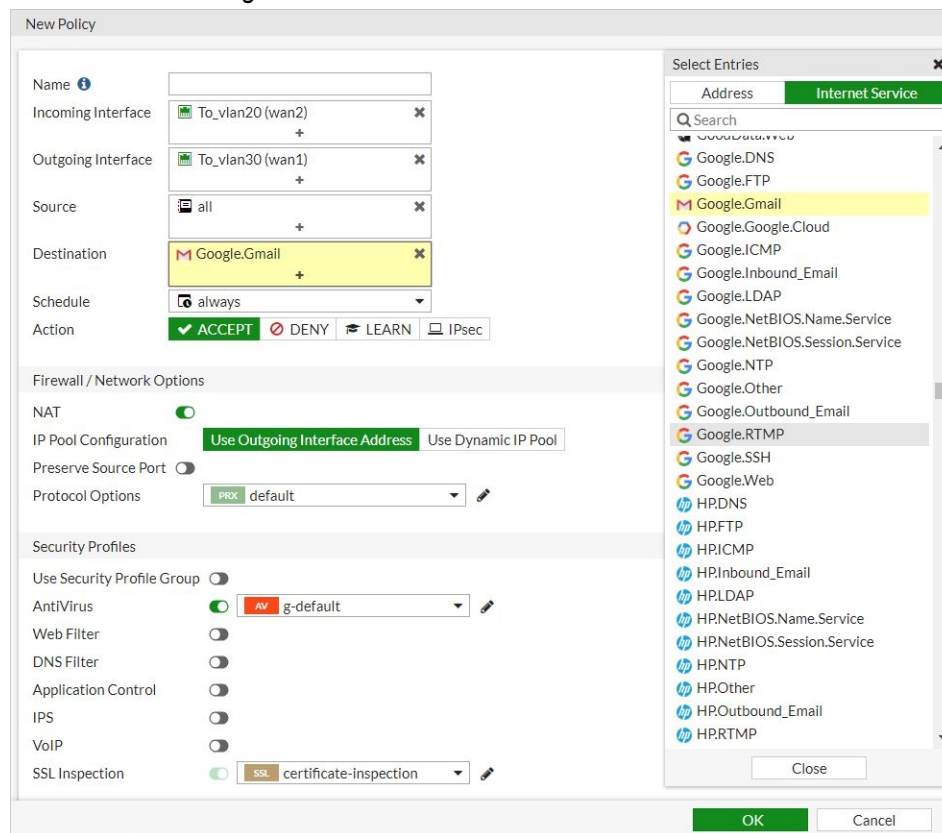
There are three types of Internet Services you can apply to a firewall policy:

- Predefined Internet Services
- Custom Internet Services
- Extension Internet Services

## Sample configuration

**To apply a predefined Internet Service entry to a policy using the GUI:**

1. Go to *Policy & Objects* and create a new policy.
2. In the *Source* or *Destination* field, click +.
3. In the *Select Entries* pane, click *Internet Service*.
4. Locate and click *Google.Gmail*.



5. Configure the other fields and then click **OK**.

**To apply a predefined Internet Service entry to a policy using the CLI:**

In the CLI, enable the `internet-service` first and then use its ID to apply the policy.

This example uses Google Gmail and its ID is 65646. Each Internet Service has a unique ID.

```
config firewall policy
 edit 9
 set name "Internet Service in Policy"
 set srcintf "wan2"
 set dstintf "wan1"
 set srcaddr "all"
 set internet-service enable
 set internet-service-id 65646
 set action accept
 set schedule "always"
 set utm-status enable
 set av-profile "g-default"
 set ssl-ssh-profile "certificate-inspection"
 set nat enable
 next
end
```

### To diagnose an Internet Service entry using the CLI:

```
diagnose internet-service id-summary 65646
Version: 0000600096
Timestamp: 201902111802
Total number of IP ranges: 444727
Number of Groups: 7
Group(0), Singularity(20), Number of IP ranges(142740)
Group(1), Singularity(19), Number of IP ranges(1210)
Group(2), Singularity(16), Number of IP ranges(241)
Group(3), Singularity(15), Number of IP ranges(38723)
Group(4), Singularity(10), Number of IP ranges(142586)
Group(5), Singularity(8), Number of IP ranges(5336)
Group(6), Singularity(6), Number of IP ranges(113891)
Internet Service: 65646(Google.Gmail)
Number of IP range: 60
Number of IP numbers: 322845
Singularity: 15
Reputation: 5(Known and verified safe sites such as Gmail, Amazon, eBay, etc.)
Icon Id: 510
Second Level Domain: 53(gmail.com)
Direction: dst
Data source: isdb
```

### Result

Because the IP and services related to Google Gmail on the Internet are included in this Internet Service (65646), all traffic to Google Gmail is forwarded by this policy.

## Using custom Internet Service in policy

Custom Internet Services can be created and used in firewall policies.

When creating a custom Internet Service, you must set following elements:

- IP or IP ranges
- Protocol number

- Port or port ranges
- Reputation

You must use CLI to create a custom Internet Service.

### Custom Internet Service CLI syntax

```
config firewall internet-service-custom
 edit <name>
 set comment <comment>
 set reputation {1|2|3|4|5}
 config entry
 edit <ID #>
 set protocol <number #>
 set dst <object_name>
 config port-range
 edit <ID #>
 set start-port <number #>
 set end-port <number #>
 next
 end
 next
 end
 end
end
```

### Sample configuration

#### To configure a custom Internet Service:

```
config firewall internet-service-custom
 edit "test-isdb-1"
 set comment "Test Custom Internet Service"
 set reputation 4
 config entry
 edit 1
 set protocol 6
 config port-range
 edit 1
 set start-port 80
 set end-port 443
 next
 end
 set dst "10-1-100-0"
 next
 edit 2
 set protocol 6
 config port-range
 edit 1
 set start-port 80
 set end-port 80
 next
 end
 set dst "172-16-200-0"
 next
 end
 end
```



```
 end
 next
end
```

### To apply a custom Internet Service into a policy:

```
config firewall policy
 edit 1
 set name "Internet Service in Policy"
 set srcintf "wan2"
 set dstintf "wan1"
 set srcaddr "all"
 set internet-service enable
 set internet-service-id 65646
 set internet-service-custom "test-isdb-1"
 set action accept
 set schedule "always"
 set utm-status enable
 set av-profile "g-default"
 set ssl-ssh-profile "certificate-inspection"
 set nat enable
 next
end
```

### Result

In addition to the IP address, IP address ranges, and services allowed by Google.Gmail, this policy also allows the traffic which access to 10.1.100.0/24 and TCP/80-443 and 172.16.200.0/24 and TCP/80.

## Using extension Internet Service in policy

Extension Internet Service lets you add custom or remove existing IP address and port ranges to an existing predefined Internet Service entries. Using an extension type Internet Service is actually editing a predefined type Internet Service entry and adding IP address and port ranges to it.

When creating an extension Internet Service and adding custom ranges, you must set following elements:

- IP or IP ranges
- Protocol number
- Port or port ranges

You must use CLI to add custom IP address and port entries into a predefined Internet Service.

You must use GUI to remove entries from a predefined Internet Service.

### Custom extension Internet Service CLI syntax

```
config firewall internet-service-extension
 edit <ID #>
 set comment <comment>
 config entry
 edit <ID #>
 set protocol <number #>
 set dst <object_name>
```

```
 config port-range
 edit <ID #>
 set start-port <number #>
 set end-port <number #>
 next
 end
 next
end
end
end
end
```

## Sample configuration

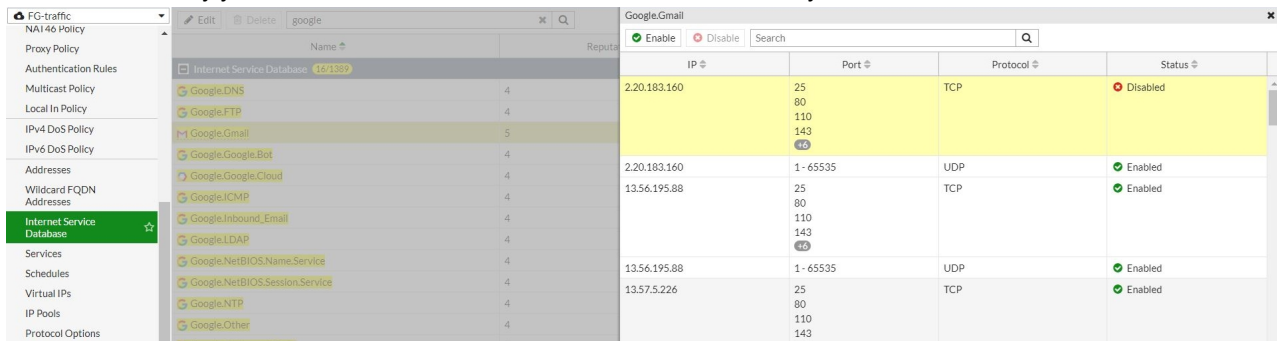
### To configure an extension Internet Service using the CLI:

```
config firewall internet-service-extension
 edit 65646
 set comment "Test Extension Internet Service 65646"
 config entry
 edit 1
 set protocol 6
 config port-range
 edit 1
 set start-port 80
 set end-port 443
 next
 end
 set dst "172-16-200-0"
 next
 edit 2
 set protocol 17
 config port-range
 edit 1
 set start-port 53
 set end-port 53
 next
 end
 set dst "10-1-100-0"
 next
 end
 next
end
next
end
```

### To remove IP address and port entries from an existing Internet Service:

1. Go to *Policy & Objects > Internet Service Database*.
2. Search for *Google.Gmail*.
3. Select *Google.Gmail* and click *Edit*.

4. Locate the *IP* entry you want to remove and click *Disable* beside that entry.



5. Click *Return*.

6. When you complete the actions in the GUI, the CLI automatically generates the configuration from your GUI actions:

```
config firewall internet-service-extension
 edit 65646
 set comment "Test Extension Internet Service 65646"
 config entry
 edit 1
 set protocol 6
 config port-range
 edit 1
 set start-port 80
 set end-port 443
 next
 end
 set dst "172-16-200-0"
 next
 edit 2
 set protocol 17
 config port-range
 edit 1
 set start-port 53
 set end-port 53
 next
 end
 set dst "10-1-100-0"
 next
 end
config disable-entry
 edit 1
 set protocol 6
 config port-range
 edit 1
 set start-port 25
 set end-port 25
 next
 edit 2
 set start-port 80
 set end-port 80
 next
 edit 3
 set start-port 110
 set end-port 110
 next
 end
 end
```

```
 next
 edit 4
 set start-port 143
 set end-port 143
 next
 edit 5
 set start-port 443
 set end-port 443
 next
 edit 6
 set start-port 465
 set end-port 465
 next
 edit 7
 set start-port 587
 set end-port 587
 next
 edit 8
 set start-port 993
 set end-port 993
 next
 edit 9
 set start-port 995
 set end-port 995
 next
 edit 10
 set start-port 2525
 set end-port 2525
 next
 end
 config ip-range
 edit 1
 set start-ip 2.20.183.160
 set end-ip 2.20.183.160
 next
 end
next
end
next
end
next
end
```

### **To apply an extension Internet Service into policy using the CLI:**

```
config firewall policy
 edit 9
 set name "Internet Service in Policy"
 set srcintf "wan2"
 set dstintf "wan1"
 set srcaddr "all"
 set internet-service enable
 set internet-service-id 65646
 set action accept
 set schedule "always"
 set utm-status enable
 set av-profile "g-default"
 set ssl-ssh-profile "certificate-inspection"
```

```
 set nat enable
 next
end
```

## Result

In addition to the IP addresses, IP address ranges, and services allowed by Google.Gmail, this policy also allows the traffic which accesses 10.1.100.0/24 and UDP/53 and 172.16.200.0/24 and TCP/80-443. At the same time, the traffic that accesses 2.20.183.160 is dropped because this IP address and port is disabled from Google.Gmail.

## Global IP address information database

The Internet Service and IP Reputation databases download details about public IP address, including: ownership, known services, geographic location, blocklisting information, and more. The details are available in drilldown information, tooltips, and other mechanisms in the FortiView and other pages.

The global IP address database is an integrated database containing all public IP addresses, and is implemented in the Internet Service Database.

### To view the owner of the IP address:

```
(global) # get firewall internet-service-owner ?
id Internet Service owner ID.
1 Google
2 Facebook
3 Apple
4 Yahoo
5 Microsoft
.....
115 Cybozu
116 VNC
```

### To check for any known service running on an IP address:

```
(global) # diagnose internet-service info FG-traffic 6 80 8.8.8.8
Internet Service: 65537(Google.Web)
```

### To check GeoIP location and blocklist information:

```
(global) # diagnose internet-service id 65537 | grep 8.8.8.8
```

### To check a known malicious server:

```
(global) # diagnose internet-service id-summary 3080383
Version: 0000600096
Timestamp: 201902111802
Total number of IP ranges: 444727
Number of Groups: 7
Group(0), Singularity(20), Number of IP ranges(142740)
Group(1), Singularity(19), Number of IP ranges(1210)
Group(2), Singularity(16), Number of IP ranges(241)
Group(3), Singularity(15), Number of IP ranges(38723)
Group(4), Singularity(10), Number of IP ranges(142586)
```

```
Group(5), Singularity(8), Number of IP ranges(5336)
Group(6), Singularity(6), Number of IP ranges(113891)
Internet Service: 3080383(Botnet.C&C.Server)
Number of IP range: 111486
Number of IP numbers: 111486
Singularity: 20
Reputation: 1(Known malicious sites related to botnet servers, phishing sites, etc.)
Icon Id: 591
Second Level Domain: 1(other)
Direction: dst
Data source: irdb
```

### To check questionable usage:

```
(global) # diagnose internet-service id-summary 2818238
Version: 0000600096
Timestamp: 201902111802
Total number of IP ranges: 444727
Number of Groups: 7
Group(0), Singularity(20), Number of IP ranges(142740)
Group(1), Singularity(19), Number of IP ranges(1210)
Group(2), Singularity(16), Number of IP ranges(241)
Group(3), Singularity(15), Number of IP ranges(38723)
Group(4), Singularity(10), Number of IP ranges(142586)
Group(5), Singularity(8), Number of IP ranges(5336)
Group(6), Singularity(6), Number of IP ranges(113891)
Internet Service: 2818238(Tor.Relay.Node)
Number of IP range: 13718
Number of IP numbers: 13718
Singularity: 20
Reputation: 2(Sites providing high risk services such as TOR, proxy, P2P, etc.)
Icon Id: 43
Second Level Domain: 1(other)
Direction: dst
Data source: irdb

(global) # diagnose internet-service id-summary 2818243
Version: 0000600096
Timestamp: 201902111802
Total number of IP ranges: 444727
Number of Groups: 7
Group(0), Singularity(20), Number of IP ranges(142740)
Group(1), Singularity(19), Number of IP ranges(1210)
Group(2), Singularity(16), Number of IP ranges(241)
Group(3), Singularity(15), Number of IP ranges(38723)
Group(4), Singularity(10), Number of IP ranges(142586)
Group(5), Singularity(8), Number of IP ranges(5336)
Group(6), Singularity(6), Number of IP ranges(113891)
Internet Service: 2818243(Tor.Exit.Node)
Number of IP range: 1210
Number of IP numbers: 1210
Singularity: 19
Reputation: 2(Sites providing high risk services such as TOR, proxy, P2P, etc.)
Icon Id: 43
Second Level Domain: 1(other)
```

```
Direction: src
Data source: irdb
```

## IP reputation filtering

There are currently five reputation levels in the Internet Service Database (ISDB), and custom reputation levels can be defined in a custom internet service. You can configure firewall policies to filter traffic according to the desired reputation level. If the reputation level of either the source or destination IP address is equal to or greater than the level set in the policy, then the packet is forwarded, otherwise, the packet is dropped.

The five default reputation levels are:

1	Known malicious sites, such as phishing sites or sites related to botnet servers
2	High risk services sites, such as TOR, proxy, and P2P
3	Unverified sites
4	Reputable social media sites, such as Facebook and Twitter
5	Known and verified safe sites, such as Gmail, Amazon, and eBay

The default minimum reputation level in a policy is zero, meaning that the reputation filter is disabled.

For IP addresses that are not included in the ISDB, the default reputation level is three.

The default reputation direction is `destination`.

### To set the reputation level and direction in a policy using the CLI:

```
config firewall policy
 edit 1
 set uuid dfcaec9c-e925-51e8-cf3e-fed9a1d42a1c
 set srcintf "wan2"
 set dstintf "wan1"
 set dstaddr "all"
 set reputation-minimum 3
 set reputation-direction source
 set action accept
 set schedule "always"
 set service "ALL"
 set logtraffic all
 set auto-asic-offload disable
 set nat enable
 next
end
```

Packets from the source IP address with reputation levels three, four, or five will be forwarded by this policy.



In a policy, if `reputation-minimum` is set, and the `reputation-direction` is `destination`, then the `dstaddr`, `service`, and `internet-service` options are removed from the policy.

If `reputation-minimum` is set, and the `reputation-direction` is `source`, then the `srcaddr`, and `internet-service-src` options are removed from the policy.

---

## Internet service groups in policies

This feature provides support for Internet Service Groups in traffic shaping and firewall policies. Service groups can be used as the source and destination of the policy. Internet Service Groups are used as criteria to match traffic; the shaper will be applied when the traffic matches.

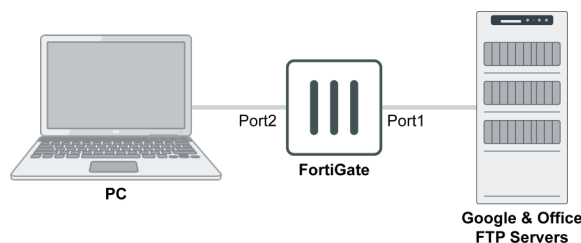
To use a group as a destination, `internet-service` must be enabled. To use a group as a source, `internet-service-src` must be enabled.

The following CLI variables are available in the `firewall policy` and `firewall shaping-policy` commands:

Variable	Description
<code>internet-service-group &lt;string&gt;</code>	Internet Service group name.
<code>internet-service-custom-group &lt;string&gt;</code>	Custom Internet Service group name.
<code>internet-service-src-group &lt;string&gt;</code>	Internet Service source group name.
<code>internet-service-src-custom-group &lt;string&gt;</code>	Custom Internet Service source group name.

### Examples

The following examples use the below topology.



### Example 1

In this example, the PC is allowed to access Google, so all Google services are put into an Internet Service Group.

**To configure access to Google services using an Internet Service Group using the CLI:**

#### 1. Create a Service Group:

```

config firewall internet-service-group
 edit "Google_Group"
 set direction destination
 set member 65537 65538 65539 65540 65542 65543 65544 65545 65550 65536 65646
 next
end

```

#### 2. Create a firewall policy to allow access to all Google Services from the PC:

```

config firewall policy
 edit 1
 set name "PC to Google"
 set srcintf "port2"

```



```

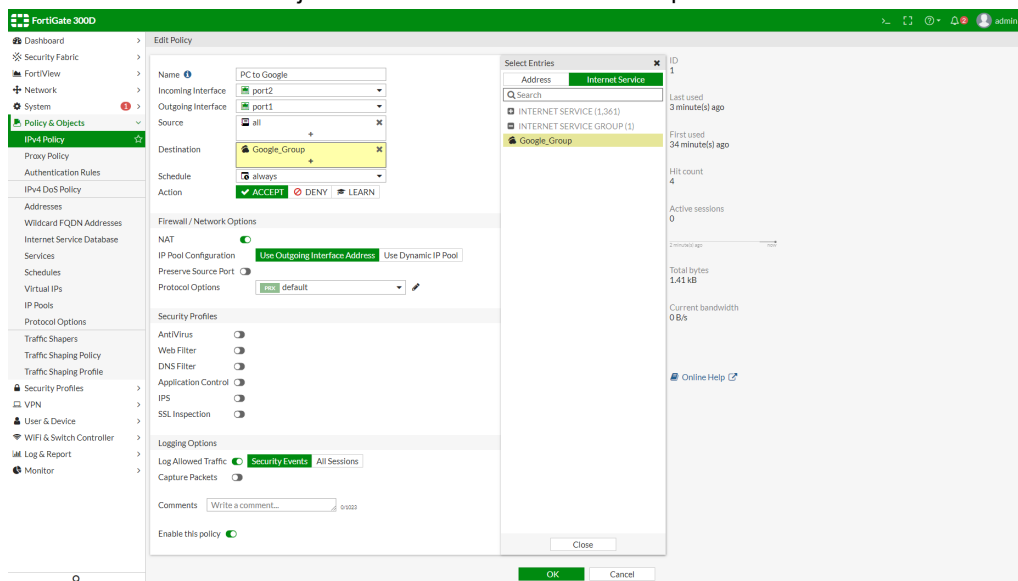
set dstintf "port1"
set srcaddr "PC"
set internet-service enable
set internet-service-group "Google_Group"
set action accept
set schedule "always"
set fsso disable
set nat enable

next
end

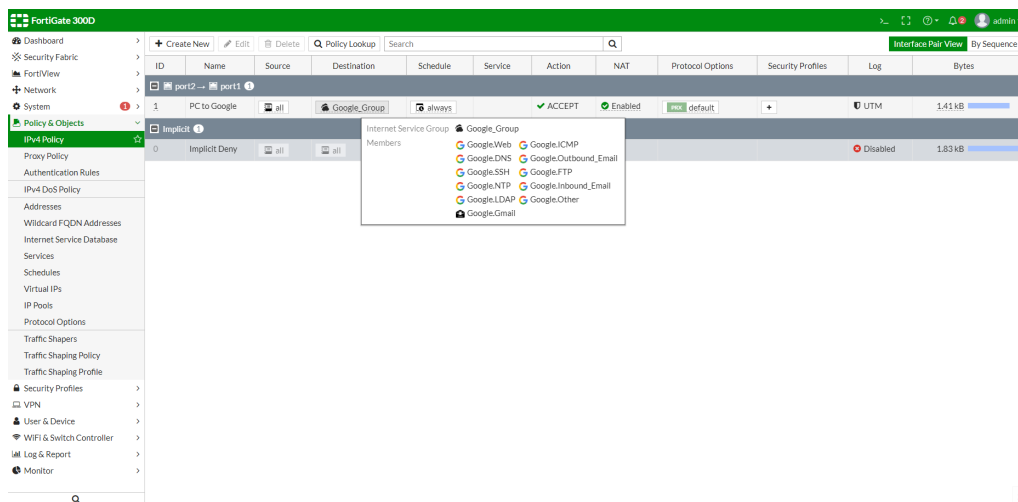
```

## To configure access to Google services using an Internet Service Group in the GUI:

1. On the FortiGate, create a Service Group using the CLI.
2. Go to *Policy & Objects* > *IPv4 Policy*, and create a new policy.
3. Set the *Destination* as the just created Internet Service Group in the GUI.



4. Configure the remaining options as shown, then click **OK**.  
On the policy page, hover over the group to view a list of its members.



## Example 2

In this example, two office FTP servers are put into an Internet Custom Service Group, and the PC connection to the FTP servers is limited to 1Mbps.

**To put two FTP servers into a custom service group and limit the PC connection speed to them using the CLI:**

1. Create custom internet services for the internal FTP servers:

```
config firewall internet-service-custom
 edit "FTP_PM"
 config entry
 edit 1
 config port-range
 edit 1
 set start-port 21
 set end-port 21
 next
 end
 set dst "PM_Server"
 next
 end
 next
edit "FTP_QA"
 config entry
 edit 1
 config port-range
 edit 1
 set start-port 21
 set end-port 21
 next
 end
 set dst "QA_Server"
 next
 end
next
end
```

2. Create a custom internet server group and add the just created custom internet services to it:

```
config firewall internet-service-custom-group
 edit "Internal_FTP"
 set member "FTP_QA" "FTP_PM"
 next
end
```

3. Create a traffic shaper to limit the maximum bandwidth:

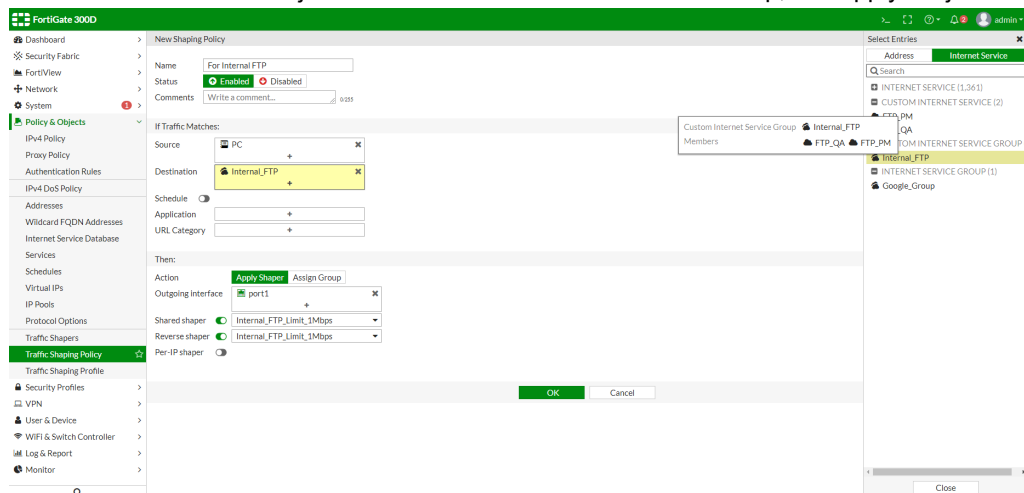
```
config firewall shaper traffic-shaper
 edit "Internal_FTP_Limit_1Mbps"
 set guaranteed-bandwidth 500
 set maximum-bandwidth 1000
 set priority medium
 next
end
```

4. Create a firewall shaping policy to limit the speed from the PC to the internal FTP servers:

```
config firewall shaping-policy
 edit 1
 set name "For Internal FTP"
 set internet-service enable
 set internet-service-custom-group "Internal_FTP"
 set dstintf "port1"
 set traffic-shaper "Internal_FTP_Limit_1Mbps"
 set traffic-shaper-reverse "Internal_FTP_Limit_1Mbps"
 set srcaddr "PC"
 next
end
```

To put two FTP servers into a custom service group and limit the PC connection speed to the using the GUI:

1. Create custom internet services for the internal FTP servers using the CLI.
2. Create a custom internet server group and add the just created custom internet services to it using the CLI.
3. Create a traffic shaper to limit the maximum bandwidth:
  - a. Go to *Policy & Objects > Traffic Shapers*, and click *Create New*.
  - b. Enter a *Name* for the shaper, such as *Internal\_FTP\_Limit\_1Mbps*.
  - c. Set the *Traffic Priority* to *Medium*.
  - d. Enable *Max Bandwidth* and set it to *1000*.
  - e. Enable *Guaranteed Bandwidth* and set it to *500*.
  - f. Click *OK*.
4. Create a firewall shaping policy to limit the speed from the PC to the internal FTP servers:
  - a. Go to *Policy & Objects > Traffic Shaping Policy*, and click *Create New*.
  - b. Set the *Destination* as the just created Custom Internet Service Group, and apply the just create traffic shaper.



- c. Configure the remaining options as shown, then click *OK*.

## Internet service customization

Internet Service Database (ISDB) entries can be tuned for their environments by adding custom ports and port ranges, as well as port mapping.

**To add a custom port range:**

```
config firewall internet-service-addition
 edit 65646
 set comment "Add custom port-range:tcp/8080-8090 into 65646"
 config entry
 edit 1
 set protocol 6
 config port-range
 edit 1
 set start-port 8080
 set end-port 8090
 next
 end
 next
 end
 next
end
```

Warning: Configuration will only be applied after rebooting or using the 'execute internet-service refresh' command.

**To verify that the change was applied:**

```
diagnose internet-service info FG-traffic 6 8080 2.20.183.160
Internet Service: 65646(Google.Gmail)
```

**To configure additional port mapping:**

```
config firewall internet-service-append
 set match-port 10
 set append-port 20
end
```

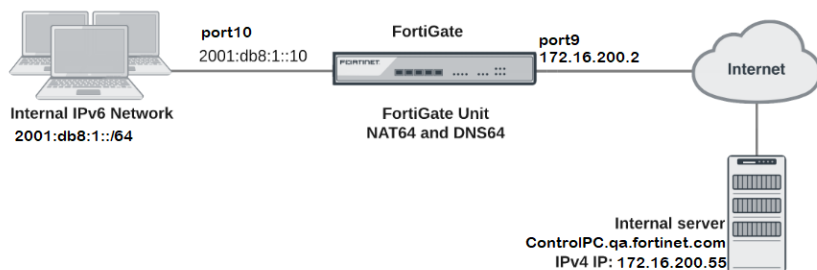
Warning: Configuration will only be applied after rebooting or using the 'execute internet-service refresh' command.

## NAT64 policy and DNS64 (DNS proxy)

NAT64 policy translates IPv6 addresses to IPv4 addresses so that a client on an IPv6 network can communicate transparently with a server on an IPv4 network.

NAT64 policy is usually implemented in combination with the DNS proxy called DNS64. DNS64 synthesizes AAAA records from A records and is used to synthesize IPv6 addresses for hosts that only have IPv4 addresses. DNS proxy and DNS64 are interchangeable terms.

## Sample topology



In this example, a host on the internal IPv6 network communicates with `ControlPC.qa.fortinet.com` that only has IPv4 address on the Internet.

1. The host on the internal network does a DNS lookup for `ControlPC.qa.fortinet.com` by sending a DNS query for an AAAA record for `ControlPC.qa.fortinet.com`.
2. The DNS query is intercepted by the FortiGate DNS proxy. The DNS proxy performs an A-record query for `ControlPC.qa.fortinet.com` and gets back an RRSet containing a single A record with the IPv4 address `172.16.200.55`.
3. The DNS proxy then synthesizes an AAAA record. The IPv6 address in the AAAA record begins with the configured NAT64 prefix in the upper 96 bits and the received IPv4 address in the lower 32 bits. By default, the resulting IPv6 address is `64:ff9b::172.16.200.55`.
4. The host on the internal network receives the synthetic AAAA record and sends a packet to the destination address `64:ff9b::172.16.200.55`.
5. The packet is routed to the FortiGate internal interface (port10) where it is accepted by the NAT64 security policy.
6. The FortiGate unit translates the destination address of the packets from IPv6 address `64:ff9b::172.16.200.55` to IPv4 address `172.16.200.55` and translates the source address of the packets to `172.16.200.200` (or another address in the IP pool range) and forwards the packets out the port9 interface to the Internet.

## Sample configuration

**To enable display for IPv6, NAT46/NAT64, and DNS Database using the GUI:**

1. Go to *System > Feature Visibility*.
2. In the *Basic Features* section, enable *IPv6*.
3. In the *Additional Features* section, enable the following features:
  - *NAT46 & NAT64*
  - *DNS Database*
4. Click *Apply*.

**To enable display for IPv6, NAT46/NAT64, and DNS Database using the CLI:**

```
config system global
 set gui-ipv6 enable
end
config system settings
 set gui-nat46-64 enable
 set gui-dns-database enable
end
```

**To enable DNS proxy on the IPv6 interface using the GUI:**

1. Go to *Network > DNS Servers*.
2. In *DNS Service on Interface*, click *Create New*.
3. For *Interface*, select *port10*.
4. Click *OK*.

**To enable DNS proxy on the IPv6 interface using the CLI:**

```
config system dns-server
 edit "port10"
 set mode forward-only
 next
end
```

**To configure IPv6 DHCP server using the CLI:**

```
config system dhcp6 server
 edit 1
 set subnet 2001:db8:1::/64
 set interface "port10"
 config ip-range
 edit 1
 set start-ip 2001:db8:1::11
 set end-ip 2001:db8:1::20
 next
 end
 set dns-server1 2001:db8:1::10
 next
end
```

**To enable NAT64 and related settings using the CLI:**

Enabling NAT64 with the `config system nat64` command means that all IPv6 traffic received by the current VDOM can be subject to NAT64 if the source and destination address matches an NAT64 security policy.

By default, the setting `always-synthesize-aaaa-record` is enabled. If you disable this setting, the DNS proxy (DNS64) will attempt to find an AAAA records for queries to domain names and therefore resolve the host names to IPv6 addresses. If the DNS proxy cannot find an AAAA record, it synthesizes one by adding the NAT64 prefix to the A record.

`nat64-prefix` setting is the `nat64` prefix. By default, it is `64:ff9b::/96`.

```
config system nat64
 set status enable
end
```

**To create NAT64 policy using the GUI:**

1. Add an IPv4 firewall address for the external network.
  - a. Go to *Policy & Object > Addresses*.
  - b. Click *Create New*.
  - c. For *Name*, enter *external-net4*.
  - d. For *IP/Network*, enter *172.16.200.0/24*.

- e. For *Interface*, select *port9*.
  - f. Click OK.
2. Add an IPv6 firewall address for the internal network.
  - a. Go to *Policy & Object > Addresses*.
  - b. Click *Create New*.
  - c. Change *Category* to *IPv6 Address*.
  - d. For *Name*, enter *internal-net6*.
  - e. For *IPv6 Address*, enter *2001:db8:1::/48*.
  - f. Click OK.
3. Add an IP pool containing the IPv4 address that is used as the source address of the packets exiting port9.
  - a. Go to *Policy & Object > IP Pools*.
  - b. Click *Create New*.
  - c. For *Name*, enter *exit-pool4*.
  - d. For *External IP Range*, enter *172.16.200.200-172.16.200.210*.
  - e. Click OK.
4. Add a NAT64 policy that allows connections from the internal IPv6 network to the external IPv4 network.
  - a. Go to *Policy & Object > NAT64 Policy*.
  - b. Click *Create New*.
  - c. For *Incoming Interface*, select *port10*.
  - d. For *Outgoing Interface*, select *port9*.
  - e. For *Source Address*, select *internal-net6*.
  - f. For *Destination Address*, select *external-net4*.
  - g. Set *IP Pool Configuration* to *Use Dynamic IP Pool* and select the IP pool *exit-pool4*.
  - h. Click OK.

**To create NAT64 policy using the CLI:**

```
config firewall address
 edit "external-net4"
 set associated-interface "port9"
 set subnet 172.16.200.0 255.255.255.0
 next
end
config firewall address6
 edit "internal-net6"
 set ip6 2001:db8:1::/48
 next
end
config firewall ippool
 edit "exit-pool4"
 set startip 172.16.200.200
 set endip 172.16.200.210
 next
end
config firewall policy64
 edit 1
 set srcintf "port10"
 set dstintf "port9"
 set srcaddr "internal-net6"
 set dstaddr "external-net4"
```

```

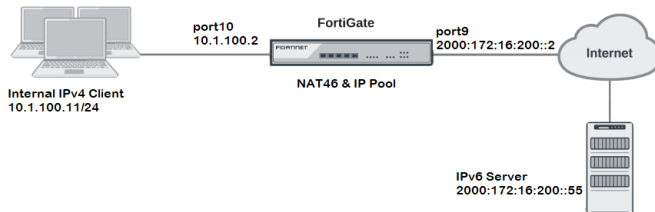
 set action accept
 set schedule "always"
 set service "ALL"
 set ippool enable
 set poolname "exit-pool4"
 next
end

```

## NAT46 policy

NAT46 refers to the mechanism that allows IPv4 addressed hosts to communicate with IPv6 hosts. Without such a mechanism, IPv4 environments cannot connect to IPv6 networks.

### Sample topology



In this example, an IPv4 client tries to connect to an IPv6 server. A VIP is configured on FortiGate to map the server IPv6 IP address 2000::172:16:200::55 to an IPv4 address 10.1.100.55. On the other side, an IPv6 IP pool is configured and the source address of packets from client are changed to the defined IPv6 address. In this setup, the client PC can access the server by using IP address 10.1.100.55.

### Sample configuration

#### To enable display for IPv6 and NAT46/NAT64 using the GUI:

1. Go to *System > Feature Visibility*.
2. In the *Basic Features* section, enable *IPv6*.
3. In the *Additional Features* section, enable *NAT46 & NAT64*.
4. Click *Apply*.

#### To enable display for IPv6 and NAT46/NAT64 using the CLI:

```

config system global
 set gui-ipv6 enable
end
config system settings
 set gui-nat46-64 enable
end

```

#### To configure VIP46 using the GUI:

1. Go to *Policy & Object > Virtual IPs*.
2. Click *Create New*.



3. For *Name*, enter *vip46\_server*.
4. For *External IP Address/Range*, enter *10.1.100.55- 10.1.100.55*.
5. For *Mapped IP Address/Range*, enter *2000:172:16:200::55*.
6. Click *OK*.

**To configure VIP46 using the CLI:**

```
config firewall vip46
 edit "vip46_server"
 set extip 10.1.100.55
 set mappedip 2000:172:16:200::55
 next
end
```

**To configure IPv6 IP pool using the GUI:**

1. Go to *Policy & Object > IP Pools*.
2. Click *Create New*.
3. For *Name*, enter *client\_external*.
4. For *External IP Range*, enter *2000:172:16:201::11- 2000:172:16:201::20*.
5. Click *OK*.

**To configure IPv6 IP pool using the CLI:**

```
config firewall ippool6
 edit "client_external"
 set startip 2000:172:16:201::11
 set endip 2000:172:16:201::20
 next
end
```

**To enable NAT64 and configure address prefix using the CLI:**

```
config system nat64
 set status enable
 set secondary-prefix-status enable
 config secondary-prefix
 edit "1"
 set nat64-prefix 2000:172:16:201::/96
 next
 end
end
```

**To create NAT46 policy using the GUI:**

1. Go to *Policy & Object > NAT46 Policy*.
2. Click *Create New*.
3. For *Incoming Interface*, select *port10*.
4. For *Outgoing Interface*, select *port9*.
5. For *Source Address*, select *all*.
6. For *Destination Address*, select *vip46\_server*.

7. Set *IP Pool Configuration to Use Dynamic IP Pool* and select the IP pool *client\_external*.
8. Click OK.

### To create NAT46 policy using the CLI:

```
config firewall policy46
 edit 1
 set srcintf "port10"
 set dstintf "port9"
 set srcaddr "all"
 set dstaddr "vip46_server"
 set action accept
 set schedule "always"
 set service "ALL"
 set ippool enable
 set poolname "client_external"
 next
end
```

## Sample troubleshooting

Example to trace flow to see the whole process.

```
diagnose debug flow filter saddr 10.1.100.11
diagnose debug flow show function-name enable
show function name
diagnose debug flow show iprope enable
show trace messages about iprope
diagnose debug flow trace start 5

id=20085 trace_id=1 func=print_pkt_detail line=5401 msg="vd-root:0 received a packet
(proto=1, 10.1.100.11:27592->10.1.100.55:2048) from port10. type=8, code=0, id=27592,
seq=1."
id=20085 trace_id=1 func=init_ip_session_common line=5561 msg="allocate a new session-
000003b9"
id=20085 trace_id=1 func=iprope_dnat_check line=4948 msg="in-[port10], out-[]"
id=20085 trace_id=1 func=iprope_dnat_tree_check line=822 msg="len=1"
id=20085 trace_id=1 func=__iprope_check_one_dnat_policy line=4822 msg="checking gnum-100000
policy-1"
id=20085 trace_id=1 func=get_vip46_addr line=998 msg="find DNAT46: IP-2000:172:16:200::55,
port-27592"
id=20085 trace_id=1 func=__iprope_check_one_dnat_policy line=4904 msg="matched policy-1,
act=accept, vip=1, flag=100, sflag=2000000"
id=20085 trace_id=1 func=iprope_dnat_check line=4961 msg="result: skb_flags-02000000, vid-1,
ret-matched, act-accept, flag-00000100"
id=20085 trace_id=1 func=fw_pre_route_handler line=183 msg="VIP-10.1.100.55:27592, outdev-
unkown"
id=20085 trace_id=1 func=__ip_session_run_tuple line=3220 msg="DNAT 10.1.100.55:8-
>10.1.100.55:27592"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2594 msg="find a route: flag=80000000
gw-10.1.100.55 via root"
id=20085 trace_id=1 func=ip4_nat_af_input line=601 msg="nat64 ipv4 received a packet
proto=1"
id=20085 trace_id=1 func=__iprope_check line=2112 msg="gnum-100012, check-fffffffa0024ebe"
id=20085 trace_id=1 func=__iprope_check_one_policy line=1873 msg="checked gnum-100012"
```

```

policy-1, ret-matched, act-accept"
id=20085 trace_id=1 func=__iprope_user_identity_check line=1677 msg="ret-matched"
id=20085 trace_id=1 func=get_new_addr46 line=1047 msg="find SNAT46: IP-2000:172:16:201::13
(from IPPPOOL), port-27592"
id=20085 trace_id=1 func=__iprope_check_one_policy line=2083 msg="policy-1 is matched, act-
accept"
id=20085 trace_id=1 func=__iprope_check line=2131 msg="gnum-100012 check result: ret-
matched, act-accept, flag-08050500, flag2-00200000"
id=20085 trace_id=1 func=iprope_policy_group_check line=4358 msg="after check: ret-matched,
act-accept, flag-08050500, flag2-00200000"
id=20085 trace_id=1 func=resolve_ip6_tuple line=4389 msg="allocate a new session-00000081"

```

## Local-in policies

While security profiles control traffic flowing through the FortiGate, local-in policies control inbound traffic that is going to a FortiGate interface.

Administrative access traffic (HTTPS, PING, SSH, and others) can be controlled by allowing or denying the service in the interface settings. Trusted hosts can be configured under an administrator to restrict the hosts that can access the administrative service.

Local-in policies allow administrators to granularly define the source and destination addresses, interface, and services. Traffic destined for the FortiGate interface specified in the policy that meets the other criteria is subject to the policies action.

Local-in policies can be used to restrict administrative access or other services, such as VPN, that can be specified as services. You can define source addresses or address groups to restrict access from. For example, by using a geographic type address you can restrict a certain geographic set of IP addresses from accessing the FortiGate.

By default, no local-in policies are defined, so there are no restrictions on local-in traffic.



Local-in policies can only be created or edited in the CLI. You can view the existing local-in policies in the GUI by enabling it in *System > Feature Visibility* under the *Additional Features* section. This page does not list the custom local-in policies.

### To configure a local-in policy using the CLI:

```

config firewall {local-in-policy | local-in-policy6}
 edit <policy_number>
 set intf <interface>
 set srcaddr <source_address> [source_address] ...
 set dstaddr <destination_address> [destination_address] ...
 set action {accept | deny}
 set service <service_name> [service_name] ...
 set schedule <schedule_name>
 set comments <string>
 next
end

```

For example, to prevent the source subnet 10.10.10.0/24 from pinging port1, but allow administrative access for PING on port1:

```

config firewall address
 edit "10.10.10.0"

```

```
 set subnet 10.10.10.0 255.255.255.0
 next
end

config firewall local-in-policy
 edit 1
 set intf "port1"
 set srcaddr "10.10.10.0"
 set dstaddr "all"
 set service "PING"
 set schedule "always"
 next
end
```

### To test the configuration:

1. From the PC at 10.10.10.12, start a continuous ping to port1:

```
ping 192.168.2.5 -t
```

2. On the FortiGate, enable debug flow:

```
diagnose debug flow filter addr 10.10.10.12
diagnose debug flow filter proto 1
diagnose debug enable
diagnose debug flow trace start 10
```

3. The output of the debug flow shows that traffic is dropped by local-in policy 1:

```
id=20085 trace_id=1 func=print_pkt_detail line=5746 msg="vd-root:0 received a packet
(proto=1, 10.10.10.12:1->192.168.2.5:2048) from port1. type=8, code=0, id=1, seq=128."
id=20085 trace_id=1 func=init_ip_session_common line=5918 msg="allocate a new session-
0017c5ad"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2615 msg="find a route:
flag=80000000 gw=192.168.2.5 via root"
id=20085 trace_id=1 func=fw_local_in_handler line=474 msg="iprope_in_check() check
failed on policy 1, drop"
```

### Additional options

To disable or re-enable the local-in policy, use the `set status {enable | disable}` command.

To dedicate the interface as an HA management interface, use the `set ha-mgmt-intf-only enable` command.

## DoS protection

A Denial of Service (DoS) policy examines network traffic arriving at a FortiGate interface for anomalous patterns, which usually indicates an attack.

A denial of service occurs when an attacking system starts an abnormally large number of sessions with a target system. The large number of sessions slows down or disables the target system, preventing legitimate users from using it.

DoS policies are checked before security policies, preventing attacks from triggering more resource intensive security protection and slowing down the FortiGate.

## DoS anomalies

Predefined sensors are setup for specific anomalous traffic patterns. New DoS anomalies cannot be added by the user.

The predefined anomalies that can be used in DoS policies are:

Anomaly	Description	Recommended Threshold
tcp_syn_flood	If the SYN packet rate of new TCP connections, including retransmission, to one destination IP address exceeds the configured threshold value, the action is executed.	2000 packets per second.
tcp_port_scan	If the SYN packet rate of new TCP connections, including retransmission, from one source IP address exceeds the configured threshold value, the action is executed.	1000 packets per second.
tcp_src_session	If the number of concurrent TCP connections from one source IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
tcp_dst_session	If the number of concurrent TCP connections to one destination IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
udp_flood	If the UDP traffic to one destination IP address exceeds the configured threshold value, the action is executed.	2000 packets per second.
udp_scan	If the UDP sessions setup rate originating from one source IP address exceeds the configured threshold value, the action is executed.	2000 sessions per second.
udp_src_session	If the number of concurrent UDP connections from one source IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
udp_dst_session	If the number of concurrent UDP connections to one destination IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
icmp_flood	If the number of ICMP packets sent to one destination IP address exceeds the configured threshold value, the action is executed.	250 packets per second.
icmp_sweep	If the ICMP sessions setup rate originating from one source IP address exceeds the configured threshold value, the action is executed.	100 sessions per second.
icmp_src_session	If the number of concurrent ICMP connections from one source IP address exceeds the configured threshold value, the action is executed.	300 concurrent sessions
icmp_dst_session	If the number of concurrent ICMP connections to one destination IP address exceeds the configured threshold value, the action is executed.	1000 concurrent sessions

Anomaly	Description	Recommended Threshold
ip_src_session	If the number of concurrent IP connections from one source IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
ip_dst_session	If the number of concurrent IP connections to one destination IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions.
sctp_flood	If the number of SCTP packets sent to one destination IP address exceeds the configured threshold value, the action is executed.	2000 packets per second
sctp_scan	If the number of SCTP sessions originating from one source IP address exceeds the configured threshold value, the action is executed.	1000 packets per second
sctp_src_session	If the number of concurrent SCTP connections from one source IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions
sctp_dst_session	If the number of concurrent SCTP connections to one destination IP address exceeds the configured threshold value, the action is executed.	5000 concurrent sessions

For thresholds based on the number of concurrent sessions, blocking the anomaly will not allow more than the number of concurrent sessions to be set as the threshold.

For example, if the period for a particular anomaly is 60 seconds, such as those where the threshold is measured in concurrent sessions, after the 60 second timer has expired the number of allowed sessions that match the anomaly criteria is reset to zero. This means that, if you allow 10 sessions through before blocking, after the 60 seconds has elapsed, another 10 sessions will be allowed. The attrition of sessions from expiration should keep the allowed sessions from reaching the maximum.

For rate based thresholds, where the threshold is measured in packets per second, the *Block* action prevents anomalous traffic from overwhelming the firewall in two ways:

- continuous: Block packets once an anomaly is detected, and continue to block packets while the rate is above the threshold. This is the default setting.
- periodical: After an anomaly is detected, allow the configured number of packets per second.

For example, if a DoS policy is configured to block icmp\_flood with a threshold of 10pps, and a continuous ping is started at a rate of 20pps for 1000 packets:

- In continuous mode, the first 10 packets are passed before the DoS sensor is triggered, and then the remaining 990 packets are blocked.
- In periodical mode, 10 packets are allowed to pass per second, so 500 packets are blocked in the 50 seconds during which the ping is occurring.



The actual numbers of passed and blocked packets may not be exact, as fluctuations in the rates can occur, but the numbers should be close to the defined threshold.

**To configure the block action for rate based anomaly sensors:**

```
config ips global
 set anomaly-mode {continuous | periodical}
end
```

**DoS policies**

A DoS policy can be configured to use one or more anomalies.

**To configure a DoS policy in the GUI:**

1. Go to *Policy & Objects > IPv4 DoS Policy* or *Policy & Objects > IPv6 DoS Policy* and click *Create New*.  
If the option is not visible, enable *DoS Policy* in *Feature Visibility*. See [Feature visibility on page 732](#) for details.
2. Configure the following:

<b>ID</b>	Enter an ID number for the policy.
<b>Incoming Interface</b>	Enter the interface that the policy applies to.
<b>Source Address</b>	Enter the source address.
<b>Destination Address</b>	Enter the destination address.  This is the address that the traffic is addressed to. In this case, it must be an address that is associated with the firewall interface. For example, it could be an interface address, a secondary IP address, or the address assigned to a VIP address.
<b>Service</b>	Select the services or service groups.  The ALL service can be used or, to optimize the firewall resources, only the services that will be answered on an interface can be used.
<b>L3 Anomalies</b> <b>L4 Anomalies</b>	Configure the anomalies: <ul style="list-style-type: none"> <li>• <i>Logging</i>: Enable/disable logging for specific anomalies or all of them. Anomalous traffic will be logged when the action is <i>Block</i> or <i>Monitor</i>.</li> <li>• <i>Action</i>: Select the action to take when the threshold is reached: <ul style="list-style-type: none"> <li>• <i>Disable</i>: Do not scan for the anomaly.</li> <li>• <i>Block</i>: Block the anomalous traffic.</li> <li>• <i>Monitor</i>: Allow the anomalous traffic, but record a log message if logging is enabled.</li> </ul> </li> <li>• <i>Threshold</i>: The number of detected instances per minute that triggers the anomaly action.</li> </ul>
<b>Comments</b>	Optionally, enter a comment.

3. Enable the policy, then click *OK*.



The quarantine option is only available in the CLI. See [Quarantine on page 827](#) for information.

**To configure a DoS policy in the GUI:**

```

config firewall DoS-policy
 edit 1
 set interface "port1"
 set srcaddr "all"
 set dstaddr "all"
 set service "ALL"
 config anomaly
 edit "icmp_flood"
 set status enable
 set log enable
 set action block
 set quarantine attacker
 set quarantine-expiry 1d1h1m
 set quarantine-log enable
 set threshold 100
 next
 end
 next
end

```

interface <string>	Enter the interface that the policy applies to.
srcaddr <string>	Enter the source address.
dstaddr <string>	Enter the destination address. This is the address that the traffic is addressed to. In this case, it must be an address that is associated with the firewall interface. For example, it could be an interface address, a secondary IP address, or the address assigned to a VIP address.
service <string>	Enter the services or service groups. The <b>ALL</b> service can be used or, to optimize the firewall resources, only the services that will be answered on an interface can be used.
status {enable   disable}	Enable/disable this anomaly.
log {enable   disable}	Enable/disable anomaly logging. When enabled, a log is generated whenever the anomaly action is triggered, regardless of which action is configured.
action {pass   block}	Set the action to take when the threshold is reached: <ul style="list-style-type: none"> <li>pass: Allow traffic, but record a log message if logging is enabled.</li> <li>block: Block traffic if this anomaly is found.</li> </ul>
quarantine {none   attacker}	Set the quarantine method (see <a href="#">Quarantine on page 827</a> ): <ul style="list-style-type: none"> <li>none: Disable quarantine.</li> <li>attacker: Block all traffic from the attacker's IP address, and add the attacker's IP address to the banned user list.</li> </ul>
quarantine-expiry <###d##h##m>	Set the duration of the quarantine, in days, hours, and minutes (###d##h##m) (1m - 364d23h59m, default = 5m). This option is available if quarantine is set attacker.



<code>quarantine-log {enable   disable}</code>	Enable/disable quarantine logging (default = disable). This option is available if quarantine is set attacker.
<code>threshold &lt;integer&gt;</code>	The number of detected instances per minute that triggers the anomaly action. The default value varies depending on the anomaly.

## Quarantine

Quarantine is used to block any further traffic from a source IP address that is considered a malicious actor or a source of traffic that is dangerous to the network. Traffic from the source IP address is blocked for the duration of the quarantine, and the source IP address is added to the banned user list.

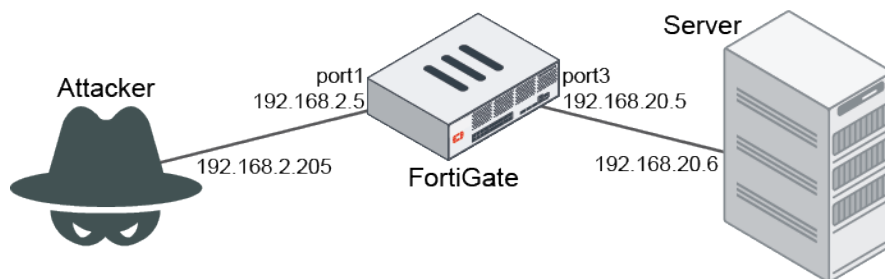
The banned user list is kept in the kernel, and used by Antivirus, Data Leak Prevention (DLP), DoS, and Intrusion Prevention System (IPS). Any policies that use any of these features will block traffic from the attacker's IP address.

### To view the quarantined user list:

```
diagnose user quarantine list
src-ip-addr created expires cause
192.168.2.205 Wed Nov 25 12:47:54 2020 Wed Nov 25 12:57:54 2020 DOS
```

## Troubleshooting DoS attacks

The best way to troubleshoot DoS attacks is with Anomaly logs and IPS anomaly debug messages.



### To test an icmp\_flood attack:

1. From the Attacker, launch an icmp\_flood with 50pps lasting for 3000 packets.
2. On the FortiGate, configure continuous mode and create a DoS policy with an icmp\_flood threshold of 30pps:

```
config firewall DoS-policy
 edit 1
 set interface "port1"
 set srcaddr "all"
 set dstaddr "all"
 set service "ALL"
 config anomaly
 edit "icmp_flood"
 set status enable
 set log enable
 set action block
 set threshold 30
 next
 next
```

```

 end
 next
end

```

### 3. Configure the debugging filter:

```

diagnose ips anomaly config
DoS sensors in kernel vd 0:
DoS id 1 proxy 0
 0 tcp_syn_flood status 0 log 0 nac 0 action 0 threshold 2000
 ...
 7 udp_dst_session status 0 log 0 nac 0 action 0 threshold 5000
 8 icmp_flood status 1 log 1 nac 0 action 7 threshold 30
 9 icmp_sweep status 0 log 0 nac 0 action 0 threshold 100
 ...
total # DoS sensors: 1.

diagnose ips anomaly filter id 8

```

### 4. Launch the icmp\_flood from a Linux machine. This example uses Nmap:

```

$ sudo nping --icmp --rate 50 -c 3000 192.168.2.50
SENT (0.0522s) ICMP [192.168.2.205 > 192.168.2.50 Echo request (type=8/code=0) id=8597
seq=1] IP [ttl=64 id=47459 iplen=28]
...
Max rtt: 11.096ms | Min rtt: 0.028ms | Avg rtt: 1.665ms
Raw packets sent: 3000 (84.000KB) | Rcvd: 30 (840B) | Lost: 2970 (99.00%)
Nping done: 1 IP address pinged in 60.35 seconds

```

### 5. During the attack, check the anomaly list on the FortiGate:

```

diagnose ips anomaly list
list nids meter:
id=icmp_flood ip=192.168.2.50 dos_id=1 exp=998 pps=46 freq=50

total # of nids meters: 1.

```

<b>id=icmp_flood</b>	The anomaly name.
<b>ip=192.168.2.50</b>	The IP address of the host that triggered the anomaly. It can be either the client or the server. For icmp_flood, the IP address is the destination IP address. For icmp_sweep, it would be the source IP address.
<b>dos_id=1</b>	The DoS policy ID.
<b>exp=998</b>	The time to be expired, in jiffies (one jiffy = 0.01 seconds).
<b>pps=46</b>	The number of packets that had been received when the diagnose command was executed.
<b>freq=50</b>	For session based anomalies, freq is the number of sessions. For packet rate based anomalies (flood, scan): <ul style="list-style-type: none"> <li>In continuous mode: freq is the greater of pps, or the number of packets received in the last second.</li> <li>In periodic mode: freq is the pps.</li> </ul>

### 6. Go to *Log & Report > Anomaly* and download the logs:

```

date=2020-11-20 time=14:38:39 eventtime=1605911919824184594 tz="-0800"
logid="0720018433" type="utm" subtype="anomaly" eventtype="anomaly" level="alert"
vd="root" severity="critical" srcip=192.168.2.205 srccountry="Reserved"
dstip=192.168.2.50 srcintf="port1" srcintfrole="undefined" sessionid=0 action="clear_session"
proto=1 service="PING" count=1307 attack="icmp_flood" icmpid="0x2195"
icmptype="0x08" icmpcode="0x00" attackid=16777316 policyid=1 policytype="DoS-policy"
ref="http://www.fortinet.com/ids/VID16777316" msg="anomaly: icmp_flood, 31 > threshold 30, repeats 28 times"
crscore=50 craction=4096 crlevel="critical"

date=2020-11-20 time=14:39:09 eventtime=1605911949826224056 tz="-0800"
logid="0720018433" type="utm" subtype="anomaly" eventtype="anomaly" level="alert"
vd="root" severity="critical" srcip=192.168.2.205 srccountry="Reserved"
dstip=192.168.2.50 srcintf="port1" srcintfrole="undefined" sessionid=0 action="clear_session"
proto=1 service="PING" count=1497 attack="icmp_flood" icmpid="0x2195"
icmptype="0x08" icmpcode="0x00" attackid=16777316 policyid=1 policytype="DoS-policy"
ref="http://www.fortinet.com/ids/VID16777316" msg="anomaly: icmp_flood, 50 > threshold 30, repeats 1497 times"
crscore=50 craction=4096 crlevel="critical"

```

## Analysis

In the first log message:

<b>msg="anomaly: icmp_flood, 31 &gt; threshold 30</b>	At the beginning of the attack, a log is recorded when the threshold of 30pps is broken.
<b>repeats 28 times</b>	The number of packets that has exceeded the threshold since the last time a log was recorded.
<b>srcip=192.168.2.205</b> <b>dstip=192.168.2.50</b>	The source and destination IP addresses of the attack.
<b>action="clear_session"</b>	Equivalent to block. If action was set to monitor and logging was enabled, this would be action="detected".

In the second log message:

- Because it is an ongoing attack, the FortiGate generates one log message for multiple packets every 30 seconds..
- It will not generate a log message if:
  - The same attack ID happened more than once in a five second period, or
  - The same attack ID happened more than once in a 30 second period and the actions are the same and have the same source and destination IP addresses.

<b>msg="anomaly: icmp_flood, 50 &gt; threshold 30</b>	In the second before the log was recorded, 50 packets were detected, exceeding the configured threshold.
<b>repeats 1497 times</b>	The number of packets that has exceeded the threshold since the last time a log was recorded

## IPv4/IPv6 access control lists

An access control list (ACL) is a granular, targeted blocklist that is used to block IPv4 and IPv6 packets on a specified interface based on the criteria configured in the ACL policy.

On FortiGate models with ports that are connected through an internal switch fabric with TCAM capabilities, ACL processing is offloaded to the switch fabric and does not use CPU resources. VLAN interfaces that are based on physical switch fabric interfaces are also supported. Interfaces that are connected through an internal switch fabric usually have names prefixed with port or lan, such as port1 or lan2; other interfaces are not supported.

The packets will be processed by the CPU when offloading is disabled or not possible, such as when a port on a supported model does not connect to the internal fabric switch.

ACL is supported on the following FortiGate models:

- 100D, 100E, 100EF, 101E
- 140D, 140D-POE, 140E, 140E-POE
- 1200D, 1500D, 1500DT
- 3000D, 3100D, 3200D, 3700D, 3800D, 3810D, 3815D
- All 300E and larger E-series models
- All 100F and larger F-series models

### Example

**To block all IPv4 and IPv6 Telnet traffic from port2 to Company\_Servers:**

```
config firewall acl
 edit 1
 set interface "port2"
 set srcaddr "all"
 set dstaddr "Company_Servers"
 set service "TELNET"
 next
end
config firewall acl6
 edit 1
 set interface "port2"
 set srcaddr "all"
 set dstaddr "Company_Servers_v6"
 set service "TELNET"
 next
end
```

### Diagnose commands

**To check the number of packets drop by an ACL:**

```
diagnose firewall acl counter
ACL id 1 dropped 0 packets

diagnose firewall acl counter6
ACL id 2 dropped 0 packets
```

**To clear the packet drop counter:**

```
diagnose firewall acl clearcounter
diagnose firewall acl clearcounter6
```

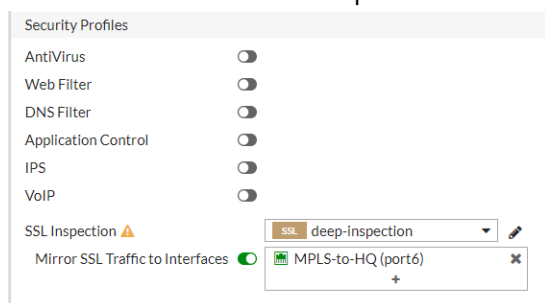
## Mirroring SSL traffic in policies

You can configure the mirroring of SSL inspected traffic for IPv4 and IPv6 policies in the GUI.

SSL inspection is automatically enabled when you enable a security profile in the policy configuration page.

**To configure mirroring of SSL traffic in a policy:**

1. Go to *Policy & Objects > IPv4 Policy* or *IPv6 Policy*.
2. Create a new policy, or edit an existing one.
3. In the *Security Profiles* section, for *SSL Inspection*, select *deep-inspection*.
4. Enable *Mirror SSL Traffic to Interfaces*. The *SSL Mirror Terms of Use* agreement appears.
5. Click *Agree* to accept the terms.
6. Select an interface from the dropdown.



7. Click *OK* to save your changes.

## Inspection mode per policy

Inspection mode is configured on a per-policy basis in NGFW mode. This gives you more flexibility when setting up different policies.

When configuring an IPv4 or IPv6 policy, you can select a *Flow-based* or *Proxy-based Inspection Mode*. The default setting is *Flow-based*.

**To configure inspection mode in a policy:**

1. Go to *Policy & Objects > IPv4 Policy* or *IPv6 Policy*.
2. Create a new policy, or edit an existing policy.

### 3. Configure the policy as needed.

- a. If you change the *Inspection Mode* to *Proxy-based*, the *Proxy HTTP(S) traffic* option displays.

The screenshot displays the FortiGate 101E configuration interface. On the left is a navigation tree with the following items: root, Dashboard, Security Fabric, FortiView, Network, System, Policy & Objects (selected), IPv4 Policy (highlighted), Proxy Policy, Authentication Rules, Multicast Policy, Local In Policy, IPv4 Access Control List, IPv4 DoS Policy, Addresses, Wildcard FQDN, Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, Traffic Shapers, Traffic Shaping Policy, Traffic Shaping Profile, Virtual Servers, and Health Check. The main panel is titled 'Edit Policy' and shows the configuration for a policy with ID 1. The configuration includes: Name (empty), Incoming Interface (wan2), Outgoing Interface (wan1), Source (all), Negate Source (disabled), Destination (all), Negate Destination (disabled), Schedule (always), Service (ALL), Action (ACCEPT, DENY, IPsec), Inspection Mode (Flow-based, Proxy-based), Proxy HTTP(S) traffic (disabled), Firewall / Network Options (NAT enabled, IP Pool Configuration: Use Outgoing Interface Address, Preserve Source Port disabled, Protocol Options: proxy default), Security Profiles (empty), and AntiVirus (disabled). At the bottom are buttons for OK and Cancel.

FortiGate 101E FortiGate-101E

root

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

IPv4 Policy

Proxy Policy

Authentication Rules

Multicast Policy

Local In Policy

IPv4 Access Control List

IPv4 DoS Policy

Addresses

Wildcard FQDN

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shapers

Traffic Shaping Policy

Traffic Shaping Profile

Virtual Servers

Health Check

Edit Policy

ID 1

Name

Incoming Interface wan2

Outgoing Interface wan1

Source all

Negate Source

Destination all

Negate Destination

Schedule always

Service ALL

Action ACCEPT DENY IPsec

Inspection Mode Flow-based Proxy-based

Proxy HTTP(S) traffic

Firewall / Network Options

NAT

IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port

Protocol Options proxy default

Security Profiles

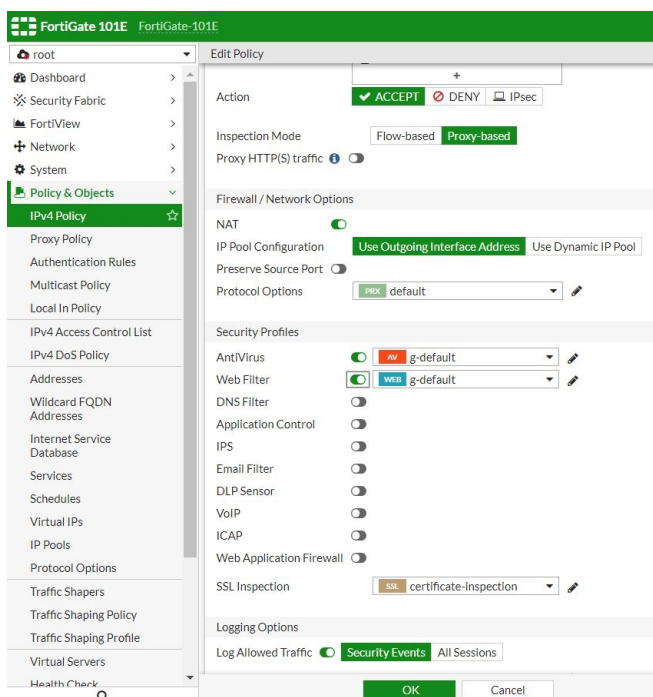
AntiVirus

OK Cancel

- b.** In the *Security Profiles* section, if no security profiles are enabled, the default *SSL Inspection* is *no-inspection*.

The screenshot displays the FortiGate 101E configuration interface. The left sidebar shows the navigation tree with 'Policy & Objects' selected. The main area shows the 'Edit Policy' configuration for 'IPv4 Policy'. The 'Action' is set to 'ACCEPT'. The 'Inspection Mode' is set to 'Proxy-based'. The 'Proxy HTTP(S) traffic' is set to 'Flow-based'. The 'Firewall / Network Objects' section shows 'NAT' is enabled, 'IP Pool Configuration' is set to 'Use Outgoing Interface Address', 'Preserve Source Port' is disabled, and 'Protocol Options' are set to 'PRIX default'. The 'Security Profiles' section lists various services like AntiVirus, Web Filter, DNS Filter, Application Control, IPS, Email Filter, DLP Sensor, VoIP, ICAP, Web Application Firewall, and SSL Inspection, all of which are currently disabled. The 'Logging Options' section shows 'Log Allowed Traffic' is enabled and 'Security Events' is selected.

- c. In the *Security Profiles* section, if you enable any security profile, the *SSL Inspection* changes to *certificate-inspection*.



To see the inspection mode changes using the CLI:

```
config firewall policy
 edit 1
 set uuid 05d88354-4817-51e9-7494-06cb70accbf0
 set srcintf "wan2"
 set dstintf "wan1"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set inspection-mode proxy
 set nat enable
 next
end
```

To see the HTTP and SSH policy redirect settings when inspection mode is set to proxy using the CLI:

```
config firewall policy
 edit 1
 set uuid 05d88354-4817-51e9-7494-06cb70accbf0
 set srcintf "wan2"
 set dstintf "wan1"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set inspection-mode proxy
```

```

set http-policy-redirect enable
set ssh-policy-redirect enable
set nat enable
next
end

```

To see the default SSL-SSH policy set to no inspection using the CLI:

```

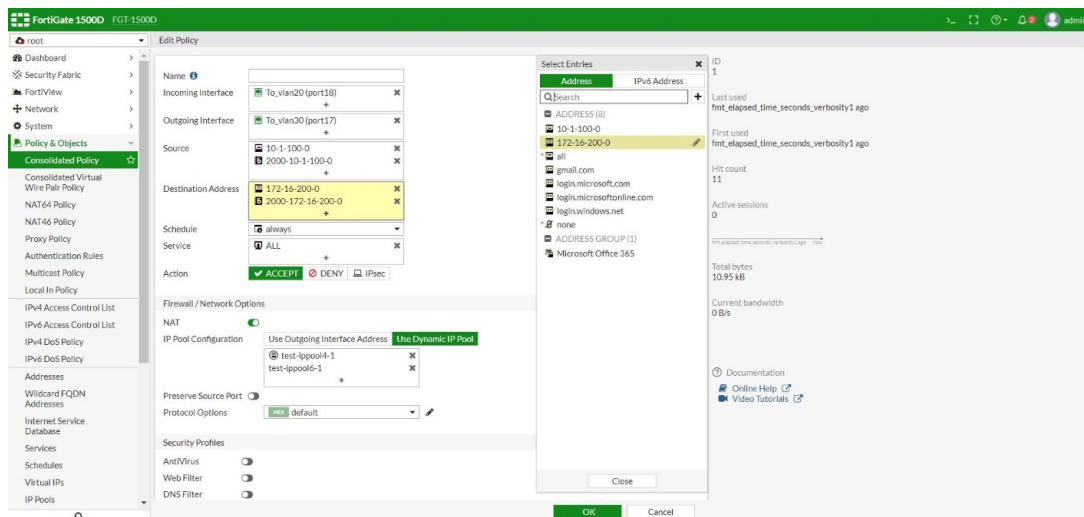
config firewall policy
edit 1
show fu | grep ssl-ssh-profile
set ssl-ssh-profile "no-inspection"
next
end

```

## Combined IPv4 and IPv6 policy

In consolidated policy mode, IPv4 and IPv6 policies are combined into a single policy instead of defining separate policies.

There is a single policy table for the GUI. The same source interface, destination interface, service, user, and schedule are shared for IPv4 and IPv6, while there are different IP addresses and IP pool settings.



To enable consolidated policy mode using the CLI:



Enabling consolidated policy mode will delete all existing IPv4 and IPv6 policies.

```

config system settings
set consolidated-firewall-mode enable
Enabling consolidated-firewall-mode will delete all firewall policy/policy6. Do you
want to continue? (y/n) y
end

```



**To configure a consolidated policy using the CLI:**

```
config firewall consolidated policy
edit 1
 set uuid 754a86b6-2507-51e9-ef0d-13a6e4bf2e9d
 set srcintf "port18"
 set dstintf "port17"
 set srcaddr4 "10-1-100-0" <----- IPv4 srcaddr
 set dstaddr4 "172-16-200-0" <----- IPv4 dstaddr
 set srcaddr6 "2000-10-1-100-0" <----- IPv6 srcaddr
 set dstaddr6 "2000-172-16-200-0" <----- IPv6 dstaddr
 set action accept
 set schedule "always"
 set service "ALL"
 set logtraffic all
 set ippool enable
 set poolname4 "test-ippool4-1" <----- IPv4 poolname
 set poolname6 "test-ippool6-1" <----- IPv6 poolname
 set nat enable
next
end
```

**Limitations**

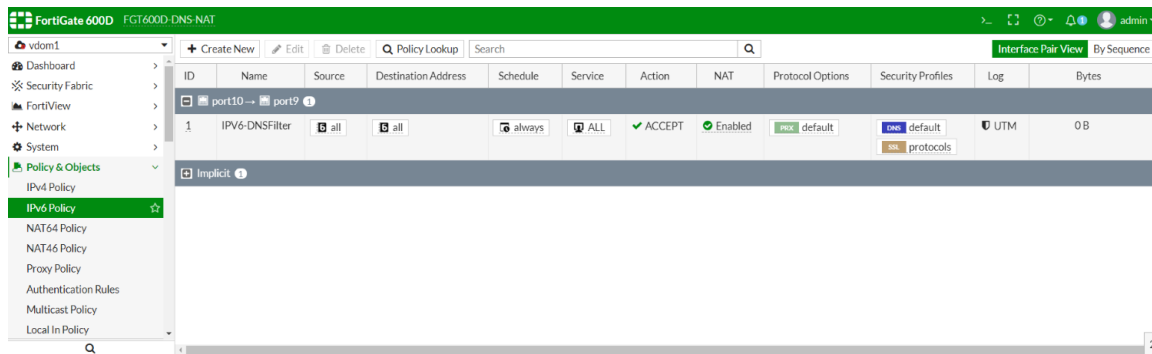
The following features are not currently supported by consolidated policy mode:

- *Internet Services* entries
- address-negate and service-negate
- DSCP and ToS matching
- Traffic shapers
- Packet capture
- External IP lists
- schedule-timeout, block-notification, disclaimer, custom-log-fields, or reputation
- timeout-send-rst, tcp-session-without-syn, or anti-replay
- *Interface Pair View* function in the pane toolbar
- *Policy Lookup* function in the pane toolbar

The session/iprope tables for IPv4 and IPv6 still display separately.

**FortiGuard DNS filter for IPv6 policies**

You can add DNS filter profile inspection to IPv6 policies. This includes FortiGuard DNS filtering (with a web filtering license) and portal replacement message redirect.



### To apply a DNS filter profile to an IPv6 policy using the CLI:

```
config firewall policy6
edit 1
 set name "IPv6-DNSFilter"
 set uuid bladb096-1919-51e9-05c7-87813d4e2b2a
 set srcintf "port10"
 set dstintf "port9"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set utm-status enable
 set dnsfilter-profile "default"
 set ssl-ssh-profile "protocols"
 set nat enable
next
end
```

A new CLI variable is added to the DNS filter profile for the IPv6 address of the SDNS redirect portal, `redirect-portal6`:

```
config dnsfilter profile
edit "default"
 set comment "Default dns filtering."
 config domain-filter
 unset domain-filter-table
 end
 config ftgd-dns
 unset options
 config filters
 edit 1
 set category 2
 set action monitor
 next
 edit 2
 set category 7
 set action monitor
 next

 end
 set log-all-domain disable
 set sdns-ftgd-err-log enable
 set sdns-domain-log enable
```

```
 set block-action redirect
 set block-botnet enable
 set safe-search disable
 set redirect-portal 0.0.0.0
 set redirect-portal6 ::
 next
end
```

After the FortiGate successfully initializes communication with the SDNS server (for the domain rating service), the following CLI command shows the default redirect portal IPv6 address:

```
(global) # diagnose test application dnsproxy 3
.....
FGD_REDIR_V4:208.91.112.55 FGD_REDIR_V6:[2001:cdba::3257:9652]
```

## OSPFv3 neighbor authentication

OSPFv3 neighbor authentication is available for enhanced IPv6 security.

### To configure an OSPF6 interface:

```
config router ospf6
 config ospf6-interface
 edit <name>
 set authentication {none | ah | esp | area}
 set key-rollover-interval <integer>
 set ipsec-auth-alg {md5 | sha1 | sha256 | sha384 | sha512}
 set ipsec-enc-alg {null | des | 3des | aes128 | aes192 | aes256}
 config ipsec-keys
 edit <spi>
 set auth-key <string>
 set enc-key <string>
 next
 end
 next
 end
end
```

### To configure an OSPF6 virtual link:

```
config router ospf6
 config area
 edit <id>
 config virtual-link
 edit <name>
 set authentication {none | ah | esp | area}
 set key-rollover-interval <integer>
 set ipsec-auth-alg {md5 | sha1 | sha256 | sha384 | sha512}
 set ipsec-enc-alg {null | des | 3des | aes128 | aes192 | aes256}
 config ipsec-keys
 edit <spi>
 set auth-key <string>
 set enc-key <string>
 next
 end
 next
 end
 end
 end
```

```

 next
 end
 next
end
end

```

### To configure an OSPF6 area:

```

config router ospf6
 config area
 edit <id>
 set authentication {none | ah | esp}
 set key-rollover-interval <integer>
 set ipsec-auth-alg {md5 | sha1 | sha256 | sha384 | sha512}
 set ipsec-enc-alg {null | des | 3des | aes128 | aes192 | aes256}
 config ipsec-keys
 edit <spi>
 set auth-key <string>
 set enc-key <string>
 next
 end
 next
 end
end
end

```

### CLI command descriptions

Command	Description
<id>	Area entry IP address.
authentication {none   ah   esp   area}	Authentication mode: <ul style="list-style-type: none"> <li>• none: Disable authentication</li> <li>• ah: Authentication Header</li> <li>• esp: Encapsulating Security Payload</li> <li>• area: Use the routing area authentication configuration</li> </ul>
key-rollover-interval <integer>	Enter an integer value (300 - 216000, default = 300).
ipsec-auth-alg {md5   sha1   sha256   sha384   sha512}	Authentication algorithm.
ipsec-enc-alg {null   des   3des   aes128   aes192   aes256}	Encryption algorithm.
<spi>	Security Parameters Index.
auth-key <string>	Authentication key should be hexadecimal numbers. Key length for each algorithm: <ul style="list-style-type: none"> <li>• MD5: 16 bytes</li> <li>• SHA1: 20 bytes</li> <li>• SHA256: 32 bytes</li> <li>• SHA384: 48 bytes</li> <li>• SHA512: 84 bytes</li> </ul>

Command	Description
	If the key is shorter than the required length, it will be padded with zeroes.
enc-key <string>	<p>Encryption key should be hexadecimal numbers.</p> <p>Key length for each algorithm:</p> <ul style="list-style-type: none"> <li>• DES: 8 bytes</li> <li>• 3DES: 24 bytes</li> <li>• AES128: 16 bytes</li> <li>• AES192: 24 bytes</li> <li>• AES256: 32 bytes</li> </ul> <p>If the key is shorter than the required length, it will be padded with zeroes.</p>

## Firewall anti-replay option per policy

When the global anti-replay option is disabled, the FortiGate does not check TCP flags in packets. The per policy anti-replay option overrides the global setting. This allows you to control whether or not TCP flags are checked per policy.

**To enable the anti-replay option so TCP flags are checked using the CLI:**

```
config firewall policy
 edit 1
 set name "policyid-1"
 set uuid dfcaec9c-e925-51e8-cf3e-fed9a1d42a1c
 set srcintf "wan2"
 set dstintf "wan1"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set anti-replay enable
 set logtraffic all
 set nat enable
 next
end
```

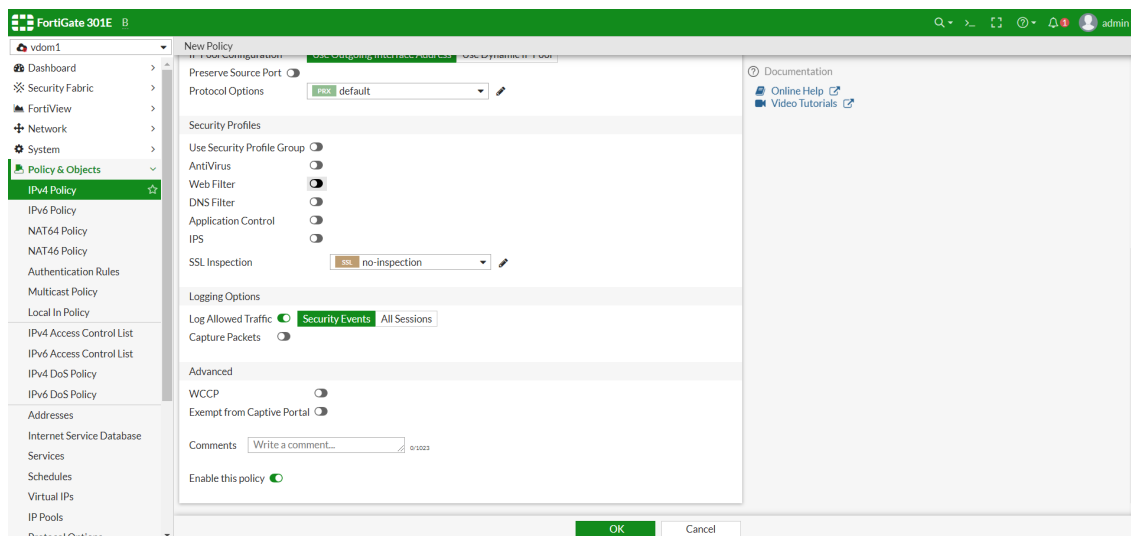
## Enabling advanced policy options in the GUI

Advanced policy options can be enabled so you can configure the options in the GUI.

**To enable advanced policy options:**

```
config system settings
 set gui-advanced-policy enable
end
```

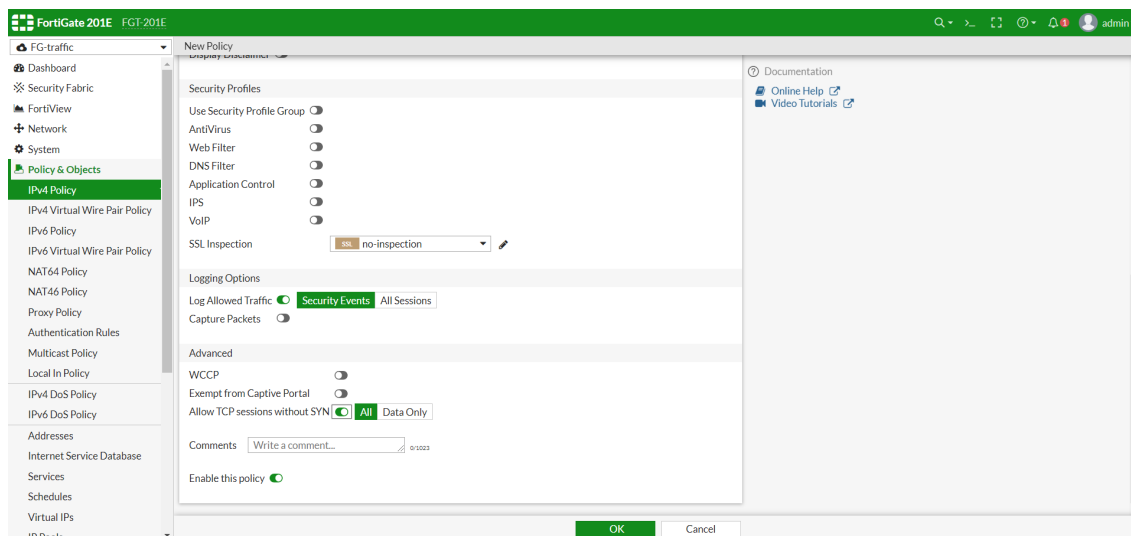
Advanced policy options are now available when creating or editing a policy in the GUI:



### To enable configuring TCP sessions without SYN:

```
config system settings
 set tcp-session-without-syn enable
end
```

TCP sessions without SYN can now be configured when creating or editing a policy in the GUI:



## Recognize anycast addresses in geo-IP blocking

An anycast IP can be advertised from multiple locations and the router selects a path based on latency, distance, cost, number of hops, and so on. This technique is widely used by providers to route users to the closest server. Since the IP is hosted in multiple geographic locations, there is no way to specify one single location to that IP.

In FortiOS 6.2.15, there is an option to bypass anycast IP ranges in geo-IP blocking. The ISDB contains a list of confirmed anycast IP ranges that can be used for this purpose.

When the source or destination is set to `geoip`, you can enable the `geoip-anycast` option. Once enabled, IPs where the anycast option is set to 1 in `geoip_db` are bypassed in country matching and blocking.



You can only use the CLI to configure this feature.

### To enable the `geoip-anycast` option using the CLI:

```
config firewall policy
 edit 1
 set name "policyid-1"
 set uuid dfcaec9c-e925-51e8-cf3e-fed9a1d42a1c
 set srcintf "wan2"
 set dstintf "wan1"
 set srcaddr "all"
 set dstaddr "test-geoip-CA_1"
 set action accept
 set schedule "always"
 set service "ALL"
 set geoip-anycast enable
 set logtraffic all
 set nat enable
 next
end
```

### To check the `geoip-anycast` option for an IP address using the CLI:

```
diagnose geoip ip2country 1.0.0.1
1.0.0.1 - Australia, is anycast ip
```

The anycast IP is 1.0.0.1.

## Authentication policy extensions

By default, unauthenticated traffic is permitted to fall to the next policy. This means that unauthenticated users are only forced to authenticate against a policy when there are no other matching policies. To avoid this, you can force authentication to always take place.

### To set that authentication requirement:

```
config user setting
 set auth-on-demand {always | implicitly}
end
```

Where:

<code>always</code>	Always trigger firewall authentication on demand.
<code>implicitly</code> (default)	Implicitly trigger firewall authentication on demand. This is the default setting (and the behavior in FortiOS 6.0 and earlier).

In the following example, authentication is required; traffic that would otherwise be allowed by the second policy is instead blocked by the first policy.

**To use forced authentication:**

```
config user setting
 set auth-on-demand always
end

config firewall policy
 edit 1
 set name "QA to Database"
 set srcintf "port10"
 set dstintf "port9"
 set srcaddr "QA_subnet"
 set dstaddr "Database"
 set action accept
 set schedule "always"
 set service "ALL"
 set fsso disable
 set groups "qa_group"
 set nat enable
 next
 edit 2
 set name "QA to Internet"
 set srcintf "port10"
 set dstintf "port9"
 set srcaddr "QA_subnet"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set fsso disable
 set nat enable
 next
end
```

## NTLM extensions

In FortiOS, agentless Windows NT LAN Manager (NTLM) authentication includes support for the following items:

- Multiple servers
- Individual users

You can use multiple domain controller servers for the agentless NTLM. They can be used for load balancing and high service stability.

You can also use user-based matching in groups for Kerberos and agentless NTLM. In these scenarios, FortiOS matches the user's group information from an LDAP server.

**To support multiple domain controllers for agentless NTLM using the CLI:****1. Configure an LDAP server:**

```
config user ldap
 edit "ldap-kerberos"
```



```
 set server "172.18.62.177"
 set cnid "cn"
 set dn "dc=fortinetqa,dc=local"
 set type regular
 set username "CN=root,CN=Users,DC=fortinetqa,DC=local"
 set password *****
 next
end
```

**2. Configure multiple domain controllers:**

```
config user domain-controller
 edit "dc1"
 set ip-address 172.18.62.177
 config extra-server
 edit 1
 set ip-address 172.18.62.220
 next
 end
 set ldap-server "ldap-kerberos"
 next
end
```

**3. Create an authentication scheme and rule:**

```
config authentication scheme
 edit "au-ntlm"
 set method ntlm
 set domain-controller "dc1"
 next
end
config authentication rule
 edit "ru-ntlm"
 set srcaddr "all"
 set ip-based disable
 set active-auth-method "au-ntlm"
 next
end
```

**4. In the proxy policy, append the user group for authorization:**

```
config firewall proxy-policy
 edit 1
 set uuid 6cfe58e4-2ff1-51e9-6b4c-a7d4a8db0f30
 set proxy explicit-web
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "all"
 set service "web"
 set action accept
 set schedule "always"
 set groups "ldap-group"
 set utm-status enable
 set av-profile "av"
 set ssl-ssh-profile "deep-custom"
 next
end
```

This configuration uses a round-robin method. When the first user logs in, the FortiGate sends the authentication request to the first domain controller. Later when another user logs in, the FortiGate sends the authentication request to another domain controller.

**5. Verify the behavior after the user successfully logs in:**

```
diagnose wad user list
ID: 1825, IP: 10.1.100.71, VDOM: vdom1
 user name : test1
 duration : 497
 auth_type : Session
 auth_method : NTLM
 pol_id : 1 g_id : 5
 user_based : 0 e
 xpire : 103
LAN:
 bytes_in=2167 bytes_out=7657
WAN:
 bytes_in=3718 bytes_out=270
```

**To support individual users for agentless NTLM using the CLI:****1. Configure an LDAP server:**

```
config user ldap
 edit "ldap-kerberos"
 set server "172.18.62.177"
 set cnid "cn"
 set dn "dc=fortinetqa,dc=local"
 set type regular
 set username "CN=root,CN=Users,DC=fortinetqa,DC=local"
 set password *****
 next
end
```

**2. Configure the user group and allow user-based matching:**

```
config user group
 edit "ldap-group"
 set member "ldap" "ldap-kerberos"
 config match
 edit 1
 set server-name "ldap-kerberos"
 set group-name "test1"
 next
 end
 next
end
```

**3. Create an authentication scheme and rule:**

```
config authentication scheme
 edit "au-ntlm"
 set method ntlm
 set domain-controller "dc1"
 next
end
config authentication rule
 edit "ru-ntlm"
 set srcaddr "all"
 set ip-based disable
 set active-auth-method "au-ntlm"
 next
end
```

**4. In the proxy policy, append the user group for authorization:**

```
config firewall proxy-policy
```

```
edit 1
 set uuid 6cfe58e4-2ff1-51e9-6b4c-a7d4a8db0f30
 set proxy explicit-web
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "all"
 set service "web"
 set action accept
 set schedule "always"
 set groups "ldap-group"
 set utm-status enable
 set av-profile "av"
 set ssl-ssh-profile "deep-custom"
next
end
```

This implementation lets you configure a single user instead of a whole group. The FortiGate will now allow the user named `test1`.

### To verify the configuration using the CLI:

```
diagnose wad user list
ID: 1827, IP: 10.1.15.25, VDOM: vdom1
user name : test1
duration : 161
auth_type : Session
auth_method : NTLM
pol_id : 1
g_id : 5
user_based : 0
expire : 439
LAN:
 bytes_in=1309 bytes_out=4410
WAN:
 bytes_in=2145 bytes_out=544
```

## HTTP to HTTPS redirect for load balancing

Starting with FortiOS 6.2.1, you can configure a virtual server with HTTP to HTTPS redirect enabled. When enabled, a virtual server can convert a client's HTTP requests to HTTPS requests. Through this mandatory conversion, HTTP traffic is converted to HTTPS traffic. This conversion improves the security of the user network.

You can only enable this feature by using the CLI. After you enable this feature, traffic flows as follows:

- When FortiGate receives an HTTP request for an external IP, such as 10.1.100.201 in the following example, FortiGate sends an HTTP 303 response back to the original client and redirects HTTP to HTTPS, instead of forwarding the HTTP request to the real backend servers.
- The client browser restarts the TCP session to HTTPS.
- The HTTPS session comes to the FortiGate where a matching IPv4 policy allows the HTTPS traffic and establishes a secure SSL connection, and then forwards the request to the real backend servers.

### To configure virtual server with HTTPS redirect enabled:

1. Create a virtual server with `server-type` set to `http`:  
`config firewall vip`

```
edit "virtual-server-http"
 set type server-load-balance
 set extip 10.1.100.201
 set extintf "wan2"
 set server-type http
 set ldb-method round-robin
 set extport 80
 config realservers
 edit 1
 set ip 172.16.200.44
 set port 80
 next
 edit 2
 set ip 172.16.200.55
 set port 80
 next
 end
end
next
end
```

- 2. Create a virtual server with server-type set to https and with the same external IP address:**

```
config firewall vip
 edit "virtual-server-https"
 set type server-load-balance
 set extip 10.1.100.201
 set extintf "wan2"
 set server-type https
 set ldb-method round-robin
 set extport 443
 config realservers
 edit 1 set ip 172.16.200.44
 set port 443
 next
 edit 2
 set ip 172.16.200.55
 set port 443
 next
 end
 set ssl-certificate "Fortinet_CA_SSL"
end
next
end
```

- 3. Enable the http-redirect option for the virtual server with server-type set to http:**

```
config firewall vip
 edit "virtual-server-http"
 set http-redirect enable
 next
end
```

- 4. Add the two virtual servers to a policy:**

```
config firewall policy
 edit 9
 set srcintf "wan2"
 set dstintf "wan1"
 set srcaddr "all"
 set dstaddr "virtual-server-http" "virtual-server-https"
 set action accept
 set schedule "always"
 set service "ALL"
```

```
set inspection-mode proxy set logtraffic all
set auto-asic-offload disable
set nat enable
next
end
```

## Use active directory objects directly in policies

Active Directory (AD) groups can be used directly in identity-based firewall policies. You do not need to add remote AD groups to local FSSO groups before using them in policies.

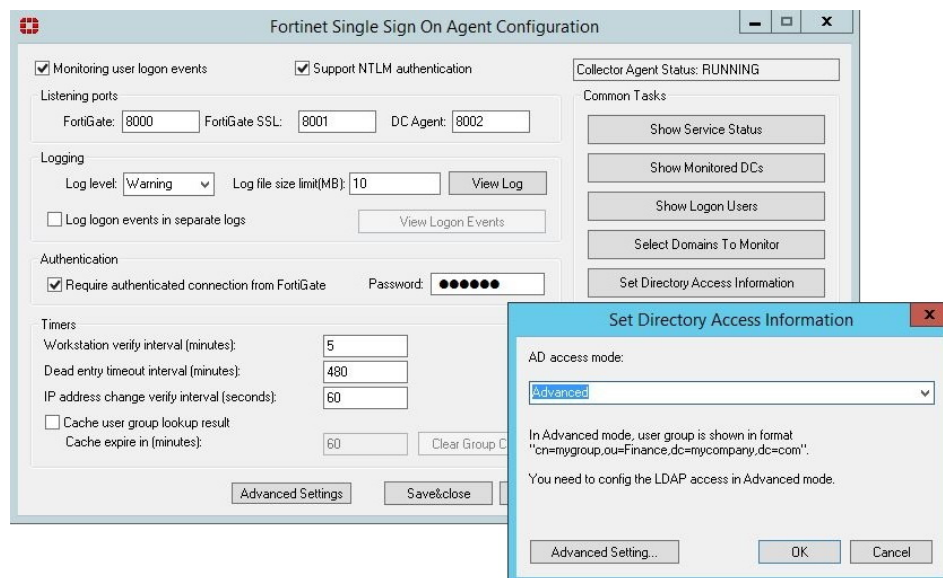
FortiGate administrators can define how often group information is updated from AD LDAP servers.

### To retrieve and use AD user groups in policies:

1. [Set the FSSO Collector Agent AD access mode on page 847](#)
2. [Add an LDAP server on page 847](#)
3. [Create the FSSO collector that updates the AD user groups list on page 848](#)
4. [Use the AD user groups in a policy on page 849](#)

## Set the FSSO Collector Agent AD access mode

To use this feature, you must set FSSO Collector Agent to *Advanced* AD access mode. If the FSSO Collector Agent is running in the default mode, FortiGate cannot correctly match user group memberships.



## Add an LDAP server

### To add an LDAP server in the GUI:

1. Go to *User & Device > LDAP Servers*.
2. Click *Create New*.

## 3. Configure the settings as needed.

## 4. If secure communication over TLS is supported by the remote AD LDAP server:

- a. Enable *Secure Connection*.
  - b. Select the protocol.
  - c. Select the certificate from the CA that issued the AD LDAP server certificate.
- If the protocol is LDAPS, the port will automatically change to 636.

## 5. Click OK.

## To add an LDAP server in the CLI:

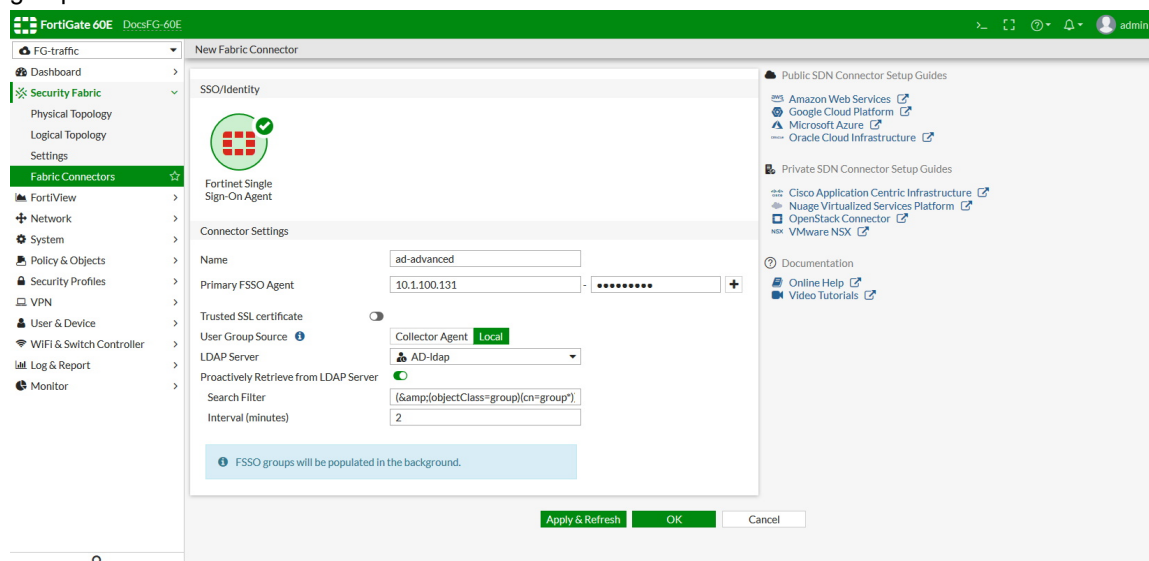
```
config user ldap
 edit "AD-ldap"
 set server "10.1.100.131"
 set cnid "cn"
 set dn "dc=fortinet-fsso,dc=com"
 set type regular
 set username "cn=Administrator,cn=users,dc=fortinet-fsso,dc=com"
 set password XXXXXXXXXXXXXXXXXXXXXXXXXX
 next
end
```

## Create the FSSO collector that updates the AD user groups list

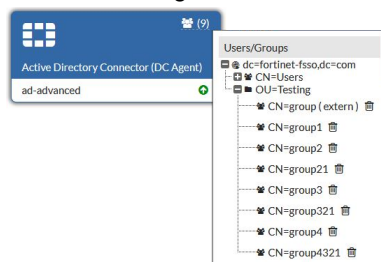
## To create an FSSO agent connector in the GUI:

1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New*.
3. In the *SSO/Identity* section, click *Fortinet Single Sign-On Agent*.
4. Fill in the *Name*.
5. Set the *Primary FSSO Agent* to the IP address of the FSSO Collector Agent, and enter its password.
6. Set the *User Group Source* to *Local*.
7. Set the *LDAP Server* to the just created *AD-ldap* server.
8. Enable *Proactively Retrieve from LDAP Server*.
9. Set the *Search Filter* to *(&(objectClass=group)(cn=group\*))*.  
The default search filter retrieves all groups, including Microsoft system groups. In this example, the filter is configured to retrieve *group1*, *group2*, etc, and not groups like *grp199*.  
The filter syntax is not automatically checked; if it is incorrect, the FortiGate might not retrieve any groups.

10. Set the *Interval (minutes)* to configure how often the FortiGate contacts the remote AD LDAP server to update the group information.



11. Click **OK**.
12. To view the AD user groups that are retrieved by the FSSO agent, hover the cursor over the group icon on the fabric connector listing.



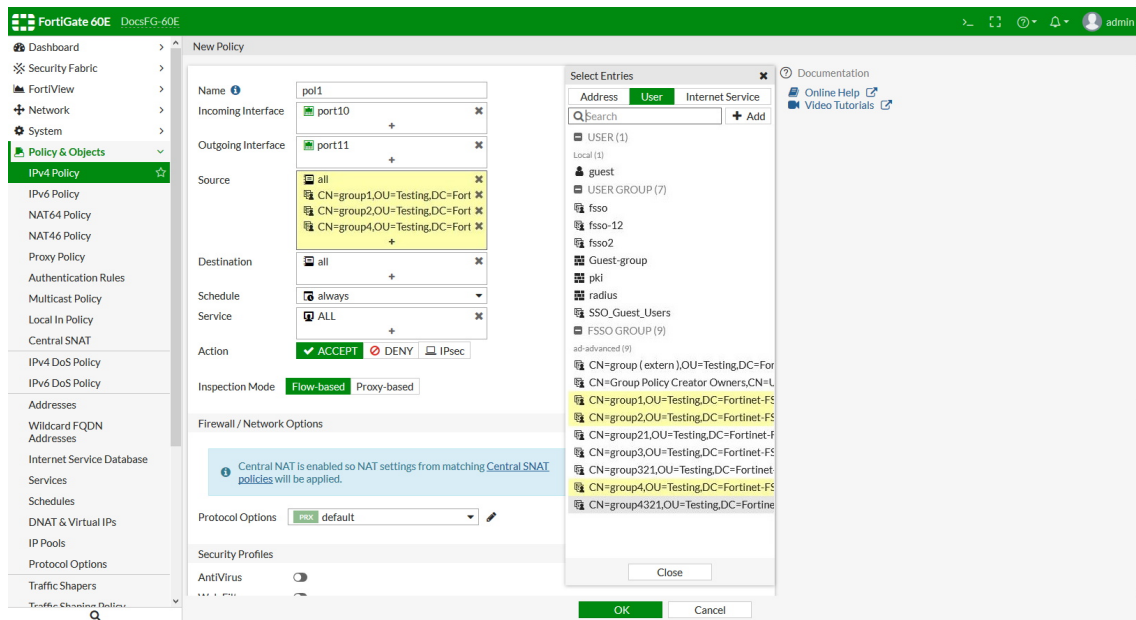
### To create an FSSO agent connector in the CLI:

```
config user fsso
 edit "ad-advanced"
 set server "10.1.100.131"
 set password XXXXXXXXXXXXXXXX
 set ldap-server "AD-ldap"
 set ldap-poll enable
 set ldap-poll-interval 2
 set ldap-poll-filter "(&(&(objectClass=group)(cn=group*)))"
 next
end
```

You view the retrieved AD user groups with the `show user adgrp` command.

### Use the AD user groups in a policy

The AD user groups retrieved by the FortiGate can be used directly in firewall policies.



## FortiGate Cloud / FDN communication through an explicit proxy

Explicit proxy communication to FortiGate Cloud and FortiGuard servers from FortiGate is enabled. A proxy server can be configured in the FortiGuard settings so that all FortiGuard connections under the `forticldd` process can be established through the proxy server.



Not all FortiGuard services are supported by these proxy settings. For example, web filter service traffic to FortiGuard will not be directed to the configured proxy.



**To configure a proxy server and communicate with FortiGate Cloud through it:**

1. Configure FortiGate B as a proxy server:

```

config firewall proxy-policy
 edit 1
 set proxy explicit-web
 set dstintf "wan1"
 set srcaddr "all"
 set dstaddr "all"
 set service "webproxy"
 set action accept
 set schedule "always"
 set logtraffic all
 set users "guest1"
 next

```



```
end
config user local
 edit "guest1"
 set type password
 set passwd 123456
 next
end
config authentication scheme
 edit "local-basic"
 set method basic
 set user-database "local-user-db"
 next
end
config authentication rule
 edit "local-basic-rule"
 set srcaddr "all"
 set ip-based disable
 set active-auth-method "local-basic"
 next
end
```

**2. Configure a firewall policy on FortiGate B to allow FortiGate A to get DNS resolution:**

```
config firewall policy
 edit 1
 set name "dns"
 set uuid c55cd2fa-9486-51e9-fc0a-c17b296f9c72
 set srcintf "port18"
 set dstintf "wan1"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "DNS"
 set fsso disable
 set nat enable
 next
end
```

**3. Configure the FortiGuard proxy settings on FortiGate A:**

```
config system fortiguard
 set proxy-server-ip 10.2.2.2
 set proxy-server-port 8080
 set proxy-username "guest1"
 set proxy-password 123456
end
```

**4. On FortiGate A, log in to FortiGate Cloud to activate the logging service:**

```
execute fortiguard-log login <username> <password>
```

**5. On FortiGate A, view the `forticldd` debug message to see the connection to the log controller through the proxy server:**

```
#
[136] fds_on_sys_fds_change: trace
[40] fds_queue_task: req-111 is added to log-controller
[596] fds_https_start_server: server: 172.16.95.168:443
```

```
[654] ssl_new: SSL object is created
[117] https_create: proxy server 10.2.2.2 port:8080
[40] fds_queue_task: req-101 is added to message-controller
[596] fds_https_start_server: server: 172.16.95.187:443
[654] ssl_new: SSL object is created
[117] https_create: proxy server 10.2.2.2 port:8080
[124] fds_on_log_setting_change: trace
[528] fds_https_connect: https_connect(172.16.95.168) is established.
[265] fds_svr_default_on_established: log-controller has connected to ip=172.16.95.168

diagnose test application forticldd 1
```

## Objects

The following topics provide information about objects:

- [Address group exclusions on page 852](#)
- [MAC addressed-based policies on page 854](#)
- [Dynamic policy — fabric devices on page 856](#)
- [FSSO dynamic address subtype on page 858](#)
- [ClearPass integration for dynamic address objects on page 862](#)
- [Using wildcard FQDN addresses in firewall policies on page 866](#)
- [VIP groups on page 869](#)

## Address group exclusions

Specific IP addresses or ranges can be subtracted from the address group with the *Exclude Members* setting in IPv4 address groups.

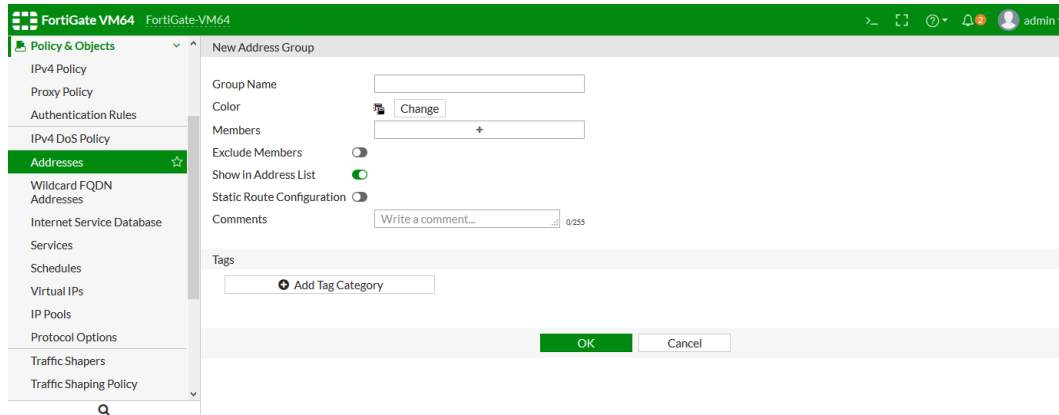


This feature is only supported for IPv4 address groups, and only for addresses with a *Type* of *IP Range* or *Subnet*.

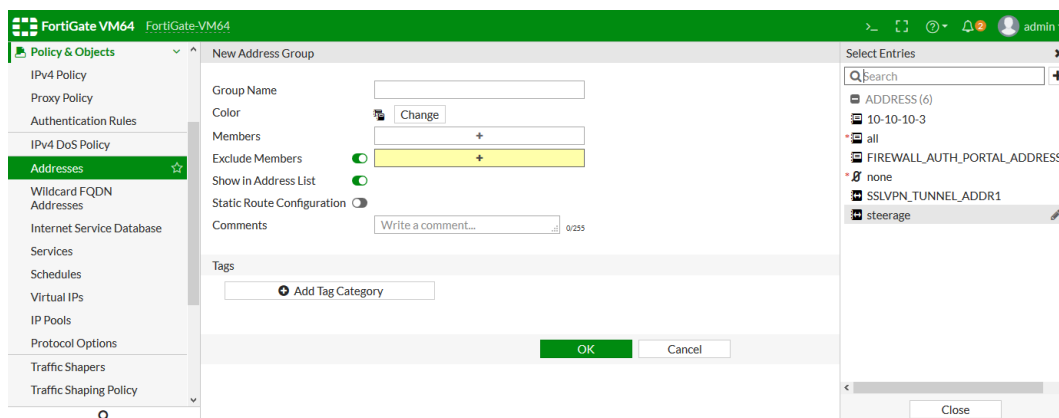
---

### To exclude addresses from an address group using the GUI:

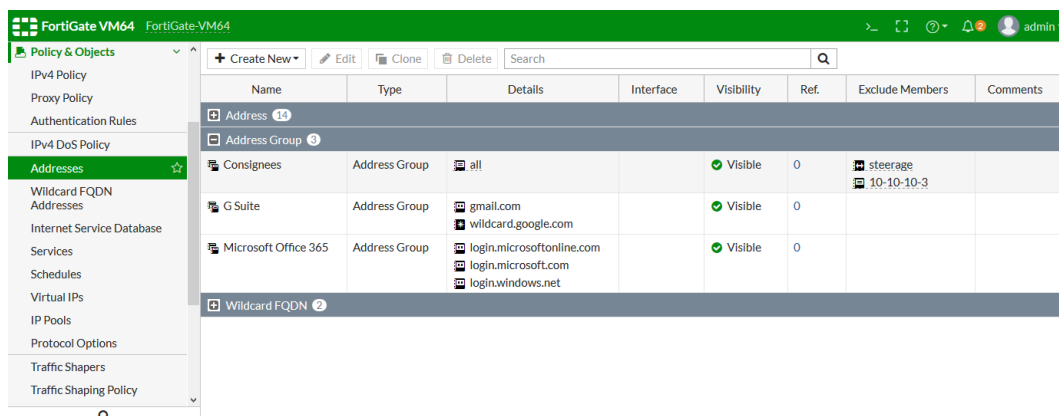
1. Go to *Policy & Objects* > *Addresses*.
2. Create a new address group, or edit an existing address group.



3. Enable *Exclude Members*. The *Select Entries* pane opens.
4. Select the addresses you want to exclude from the group.
5. Click *OK*.



The excluded members are listed in the *Exclude Members* column.



### To exclude addresses from an address group using the CLI:

```
config firewall addrgrp
```

```

edit <address group>
 set exclude enable
 set exclude-member <address> <address> ... <address>
next
end

```

## MAC addressed-based policies

MAC address ranges can be added to the following IPv4 policies:

- Firewall
- Virtual wire pair
- ACL
- Central SNAT
- DoS

A MAC address is a link layer-based address type and it cannot be forwarded across different IP segments.

FortiOS only supports the MAC address type as source address for policies in NAT mode VDOM. When you use the MAC address type in a policy as source address in NAT mode VDOM, IP address translation (NAT) is still performed according to the rules defined in the policy. The MAC address type only works for source address matching. It does not have any association with NAT actions.

For policies in transparent mode or the virtual wire pair interface, you can use the MAC address type as source or destination address.

### To configure a MAC address range using the GUI:

1. Go to *Policy & Objects > Addresses* to create or edit an address:
  - a. For *Category*, select *Address*.
  - b. For *Type*, select *MAC Address Range*.
  - c. Enter the address range in the empty fields.
  - d. Configure the other fields as needed.
  - e. Click *OK*.

The screenshot shows the FortiGate 300D GUI with the 'Edit Address' window open. The left sidebar shows the navigation menu with 'Addresses' selected. The main window has the following fields:

- Category:** Address (selected), IPv6 Address, Multicast Address, Proxy Address
- Name:** test-mac-addr1
- Color:** Change
- Type:** MAC Address Range
- MAC Address Range:** 00:0c:29:41:98:88 - 00:0c:29:41:98:88
- Interface:** any
- Show In Address List:** ☒
- Comments:** Write a comment... (0/255)
- Tags:** Select Tags

At the bottom right, there are 'OK' and 'Cancel' buttons.

2. Go to *Policy & Objects > IPv4 Policy* to apply the address type to a policy in NAT mode VDOM:

- For *Source*, select the MAC address you just configured.
- For *Destination*, select an address.



In NAT mode VDOM, this address type cannot be used as destination address.

c. Click OK.

## To configure a MAC address range using the CLI:

1. Create a new MAC address range type:

```
config firewall address
 edit <object_name>
 set type mac
 set start-mac <mac_address_start #>
 set end-mac <mac_address_end #>
 next
end
```

2. Apply the address type to a policy. In transparent mode or the virtual wire pair interface, this address type can be mixed with other address types in the policy:

```
config firewall address
 edit "test-mac-addr1"
 set type mac
 set start-mac 00:0c:29:41:98:88
 set end-mac 00:0c:29:41:98:88
 next
end
```

```

config firewall policy
 edit 1
 set srcintf "port2"
 set dstintf "port1"
 set srcaddr "test-mac-addr1" "10-1-100-42"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set logtraffic all
 set nat enable
 next
end

```

## Dynamic policy — fabric devices

The dynamic address group represents the configured IP addresses of all Fortinet devices connected to the Security Fabric. It currently includes FortiManager, FortiAnalyzer, FortiClient EMS, FortiMail, FortiAP(s), and FortiSwitch(es). Like other dynamic address groups for fabric connectors, it can be used in IPv4 policies and objects.

The list of firewall addresses includes a default address object called `FABRIC_DEVICE`. You can apply the `FABRIC_DEVICE` object to the following types of policies:

- IPv4 firewall policy (including virtual wire pairs)
- IPv4 shaping policy
- IPv4 ACL policy
- `policy64` and `policy46` (IPv4 only)
- Consolidated policy (IPv4 only)

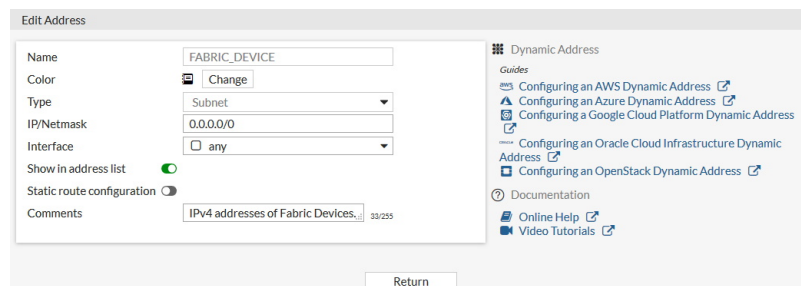
You cannot apply the `FABRIC_DEVICE` object to the following types of policies:

- All IPv6 policies
- IPv4 explicit proxy policy

You also cannot use the `FABRIC_DEVICE` object with the following settings:

- Custom extension on `internet-service`
- Exclusion of `addrgrp`

Initially the `FABRIC_DEVICE` object does not have an address value. The address value is populated dynamically as things change. As a result, you cannot edit the `FABRIC_DEVICE` object, add any addresses to the object, or remove any addresses from the object. The *Edit Address* pane in the GUI only has a *Return* button because the object is read-only:

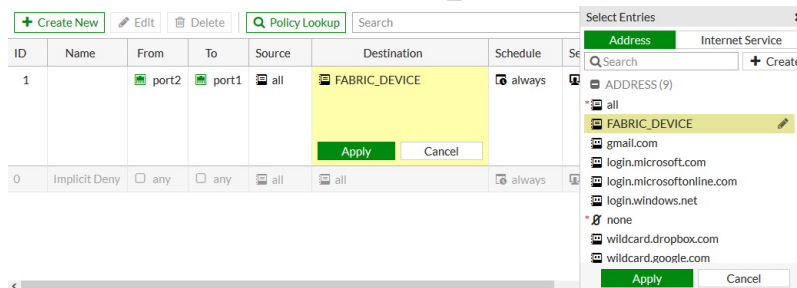


The `FABRIC_DEVICE` object address values are populated based on:

- FortiAnalyzer IP (from the *Fabric Settings* pane)
- FortiManager IP (from the *Fabric Settings* pane)
- FortiMail IP (from the *Fabric Settings* pane)
- FortiClient EMS IP (from the *Fabric Settings* pane)
- FortiAP IPs (from the *FortiAP Setup* pane or DHCP)
- FortiSwitch IPs (from the *FortiSwitch Setup* page or DHCP)

### To apply the FABRIC\_DEVICE object to an IPv4 policy using the GUI:

1. Go to *Policy & Objects > IPv4 Policy*.
2. Create a new policy or edit an existing policy.
3. For the *Destination* field, select *FABRIC\_DEVICE* from the list of address entries.



4. Configure the rest of the policy as needed.
5. Click OK.

### To apply the FABRIC\_DEVICE object to an IPv4 policy using the CLI:

```
(root) # show full-configuration firewall address FABRIC_DEVICE
config firewall address
 edit "FABRIC_DEVICE"
 set uuid ffde44a6-9eab-51ea-62f2-d5facde7af77
 set type ipmask
 set comment "IPv4 addresses of Fabric Devices."
 set associated-interface ''
 set color 0
 set allow-routing disable
 set subnet 0.0.0.0 0.0.0.0
 next
end

config firewall policy
 edit 1
 set srcintf "port2"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "FABRIC_DEVICE"
 set action accept
 set schedule "always"
 set service "ALL"
 set utm-status enable
 set fsso disable
 set nat enable
 next
end
```

## Diagnose command

You can use the diagnose command to list IP addresses of Fortinet devices that are configured in the Security Fabric.

### To run the diagnose command using the CLI:

```
(root) # diagnose firewall sf-addresses list
```

```
FabricDevices: 172.18.64.48
FortiAnalyzer: 172.18.60.25
FortiSandbox: 172.18.52.154
FortiManager: 172.18.28.31
FortiClientEMS: 172.18.62.6
FortiAP:
FortiSwitch:
FortiAP/SW-DHCP:
```

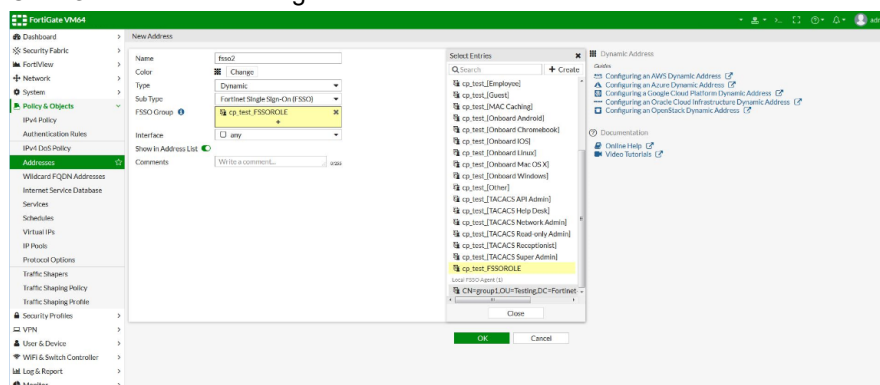
## FSSO dynamic address subtype

The Fortinet Single Sign-ON (FSSO) dynamic firewall address subtype can be used in policies that support dynamic address types. The FortiGate will update the dynamic address used in firewall policies based on the source IP information for the authenticated FSSO users.

It can also be used with FSSO group information that is forwarded by ClearPass Policy Manager (CPPM) via FortiManager, and other FSSO groups provided by the FSSO collector agent or FortiNAC.

### To configure FSSO dynamic addresses with CPPM and FortiManager in the GUI:

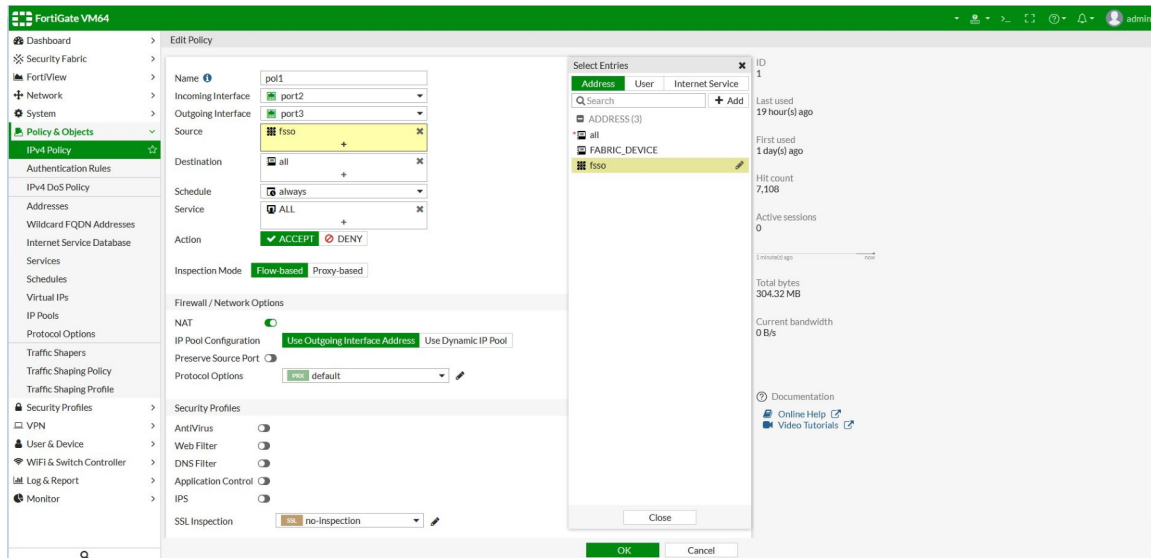
1. Create the dynamic address object:
  - a. Go to **Policy & Objects > Addresses > Create New > Address**.
  - b. For **Type**, select **Dynamic**.
  - c. For **Sub Type**, select **Fortinet Single Sign-On (FSSO)**. The **Select Entries** pane opens and displays all available FSSO groups.
  - d. Select one or more groups.
  - e. Click **OK** to save the configuration.



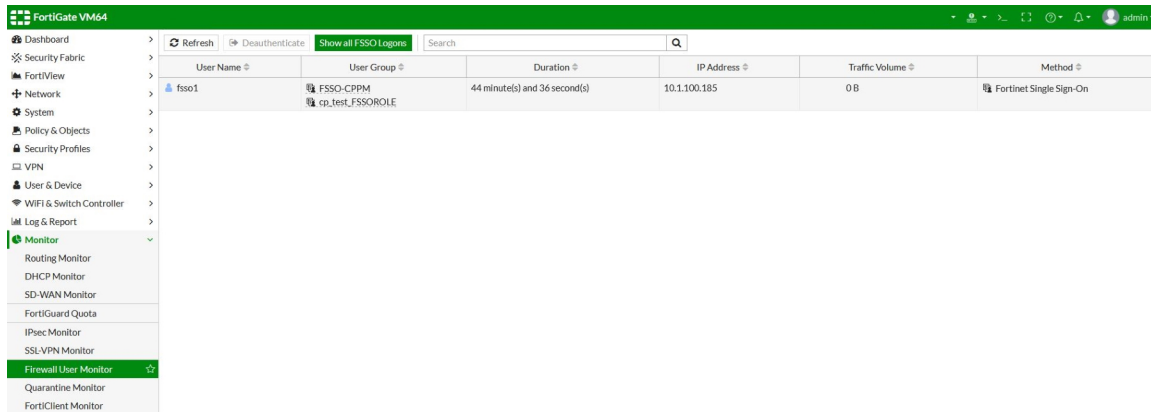
When the address table appears, there will be an error message for the address you just created (*Unresolved dynamic address: fssso*). This is expected because there are currently no authenticated FSSO users (based on source IP) in the local FSSO user list.



2. Add the dynamic address object to a firewall policy:
  - a. Go to *Policy & Objects > IPv4 Policy*.
  - b. Create a new policy or edit an existing policy.
  - c. For *Source*, add the dynamic FSSO address object you just created.
  - d. Configure the rest of the policy as needed.
  - e. Click *OK* to save your changes.

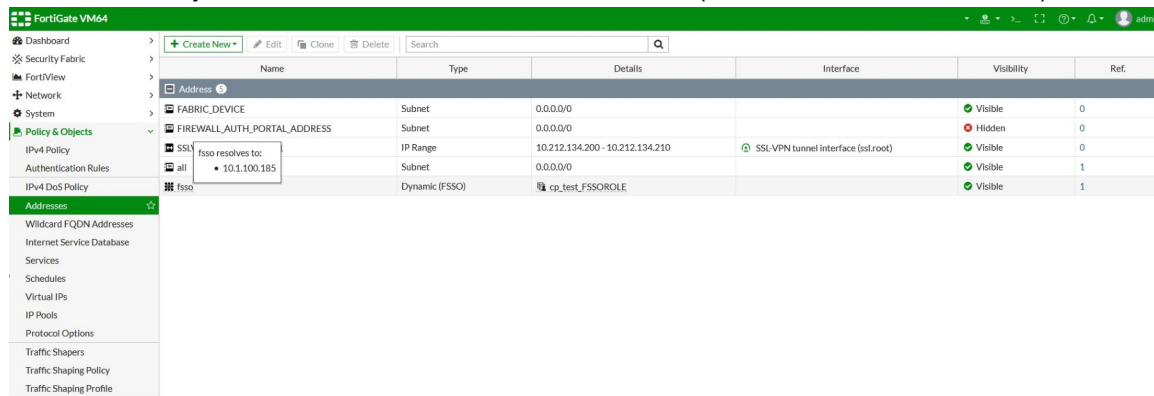


3. Test the authentication to add a source IP address to the FSSO user list:
  - a. Log in as user and use CPPM for user authentication to connect to an external web server. After successful authentication, CPPM forwards the user name, source IP address, and group membership to the FortiGate via FortiManager.
  - b. Go to *Monitor > Firewall User Monitor* to view the user name (*fssso1*) and IP address.



- c. Go to *Policy & Objects > Addresses* to view the updated address table. The error message no longer appears.

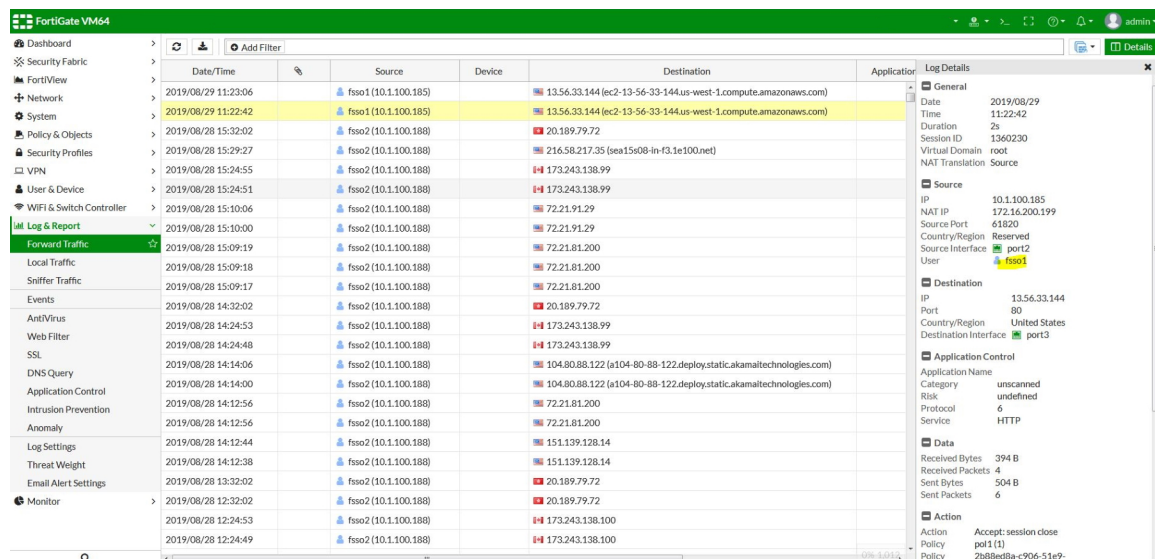
- d. Hover over the dynamic FSSO address to view the IP address (*fssso resolves to: 10.1.100.185*).



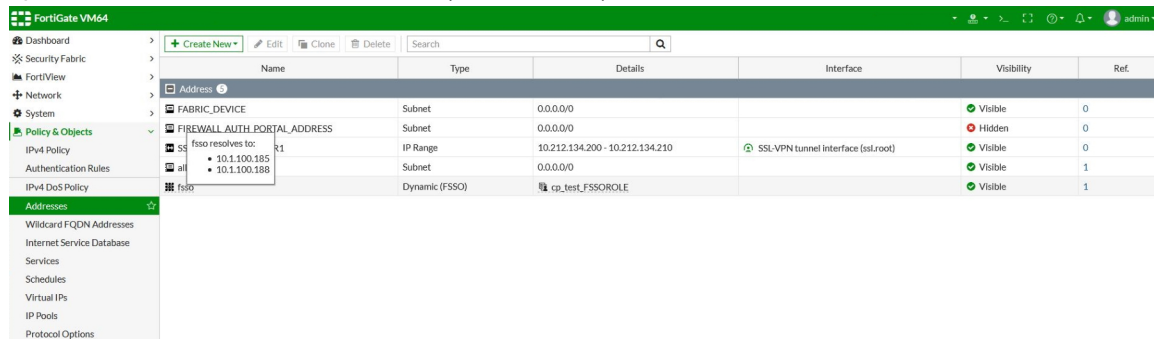
## To verify user traffic in the GUI:

- Go to **Log & Report > Forward Traffic**.

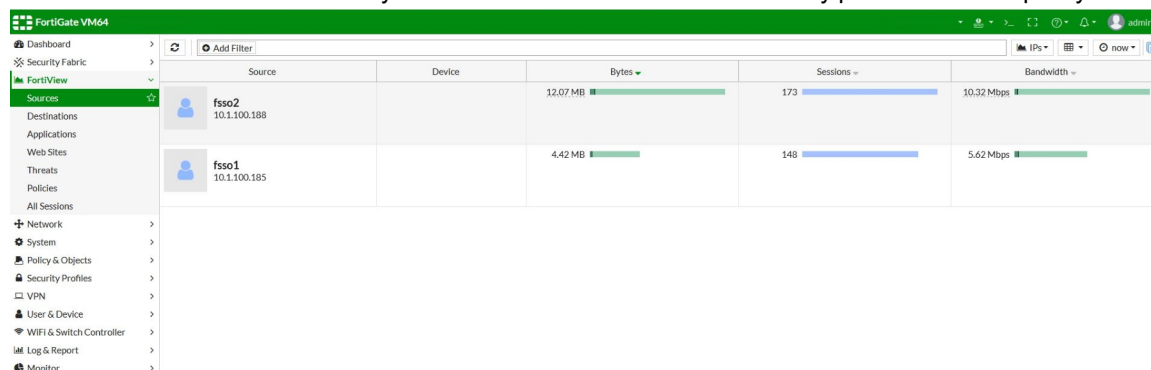
Details for the user *fssso1* are visible in the traffic log:



- If another user is authenticated by CPPM, then the dynamic address *fssso* entry in the address table will be updated. The IP address for user *fssso2* (*10.1.100.188*) is now visible:



2. Go to *FortiView* > *Sources* to verify that the users were able to successfully pass the firewall policy.



If a user logs off and CPPM receives log off confirmation, then CPPS updates the FortiGate FSSO user list via FortiManager. The user IP address is deleted from the dynamic FSSO address, and the user is no longer be able to pass the firewall policy.

## To configure FSSO dynamic addresses with CPPM and FortiManager in the CLI:

1. Create the dynamic address object:

```
config firewall address
 edit "fsso"
 set uuid 6f63c872-c90b-51e9-ebfd-16c18807c795
 set type dynamic
 set sub-type fsso
 set fsso-group "cp_test_FSSOROLE"
 next
end
```

2. Add the dynamic address object to a policy:

```
config firewall policy
 edit 1
 set name "pol1"
 set uuid 2b88ed8a-c906-51e9-fb25-8cb12172acd8
 set srcintf "port2"
 set dstintf "port3"
 set srcaddr "fsso"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set logtraffic all
 set fsso disable
 set nat enable
 next
end
```

**To verify user traffic in the CLI:****1. Check the FSSO user list:**

```
diagnose debug authd fsso list
----FSSO logons----
IP: 10.1.100.185 User: fssol Groups: cp_test_FSSOROLE Workstation: MemberOf: FSSO-
CPPM cp_test_FSSOROLE
Total number of logons listed: 1, filtered: 0
----end of FSSO logons----
```

**2. Check the authenticated firewall users list:**

```
diagnose firewall auth list
10.1.100.185, fssol
type: fsso, id: 0, duration: 2928, idled: 2928
server: FortiManager
packets: in 0 out 0, bytes: in 0 out 0
group_id: 2 33554433
group_name: FSSO-CPPM cp_test_FSSOROLE
----- 1 listed, 0 filtered -----
```

After user traffic passes through the firewall, the nu

```
diagnose firewall auth list
10.1.100.185, fssol
type: fsso, id: 0, duration: 3802, idled: 143
server: FortiManager
packets: in 1629 out 1817, bytes: in 2203319 out 133312
group_id: 2 33554433
group_name: FSSO-CPPM cp_test_FSSOROLE
----- 1 listed, 0 filtered -----
```

## ClearPass integration for dynamic address objects

ClearPass Policy Manager (CPPM) can gather information about the statuses of network hosts, for example, the latest patches or virus infections. Based on this information, CPPM send the IP addresses and current states, such as Healthy or Infected, to the FortiGate.

On the FortiGate, the IP addresses received from CPPM are added to a dynamic firewall address with the *clearpass-spt* subtype. This address can be used in any policy that supports dynamic addresses, such as Firewall or SSL-VPN policies.

In this example, you create two dynamic IP addresses that are used in two firewall policies (deny and allow). One policy allows traffic (host state = Healthy), and the other denies traffic (host state = Infected). When CPPM sends the information, the IP addresses are assigned according to their host state: Healthy or Infected.

You can then verify that traffic from the Infected host is denied access by the deny policy, and traffic from the Healthy host is allowed access by the allow policy.

## Create a REST API administrator

A RESET API administrator is required to generate an authorization token for REST API messages, and to limit hosts that can send REST API messages to the FortiGate.

### To create a REST API administrator in the GUI:

1. Go to *System > Administrators*.
2. Click *Create New > REST API Admin*.
3. Configure the *Username* and other information as needed.
4. Disable *PKI Group*.
5. In the *Trusted Hosts* field, enter *10.1.100.0/24*.

For this example, an administrator profile called *clearpass* was created with full read/write access. See [Administrator profiles on page 619](#) for details.

6. Click *OK*.  
The *New API key* pane opens.

The API key is the REST API authorization token that is used in REST API messages sent by CPPM to the FortiGate.

7. Copy the API key to a secure location. A new key can be generated if this one is lost or compromised.
8. Click *Close*.

### To create a REST API administrator in the CLI:

```
config system api-user
 edit "cp-api-back"
 set accprofile "clearpass"
 config trusthost
 edit 1
 set ipv4-trusthost 10.1.100.0 255.255.255.0
 next
 end
 next
end
```

```
execute api-user generate-key cp-api
New API key: 0f1HxGHh9r9p74k7qgfHNNH40p51bj5
NOTE: The bearer of this API key will be granted all access privileges assigned to the
api-user cp-api.
```

### Create dynamic IP addresses with the clearpass subtype

Two dynamic IP addresses are required, one for the allow policy, and the other for the deny policy.

#### To create the dynamic IP addresses:

```
config firewall address
 edit "cppm"
 set uuid 62a180c0-cb36-51e9-6e70-4a2034d82179
 set type dynamic
 set sub-type clearpass-spt
 set clearpass-spt healthy
 set comment ''
 set visibility enable
 set associated-interface ''
 set color 0
 next
 edit "cppm-deny"
 set uuid b318e962-cb36-51e9-7a34-74a34cf3bf0b
 set type dynamic
 set sub-type clearpass-spt
 set clearpass-spt infected
 set comment ''
 set visibility enable
 set associated-interface ''
 set color 0
 next
end
```

### Create firewall policies

Two firewall policies are required, one to accept traffic (*cppm-allow*), and the other to deny traffic (*cppm-deny*).

#### To create the firewall policies in the GUI:

1. Go to *Policy & Objects > IPv4 Policy*.
2. Configure the allow policy:
  - a. Click *Create New*.
  - b. Enter a name for the policy.
  - c. Set *Source* set to *cppm*.
  - d. Set *Action* to *ACCEPT*.

- e. Configure the remaining settings as needed.

The screenshot shows the 'New Policy' configuration window in the FortiGate 60E GUI. The policy is named 'cppm-allow'. The incoming interface is 'port10' and the outgoing interface is 'port9'. The source is 'cppm' and the destination is 'all'. The schedule is 'always' and the service is 'ALL'. The action is set to 'ACCEPT'. The inspection mode is 'Flow-based'. The NAT section is enabled, and the IP pool configuration is set to 'Use Outgoing Interface Address'. The security profiles section shows 'AntiVirus' set to 'AV default' and 'Web Filter' is disabled.

- f. Click OK.

### 3. Configure the deny policy:

- Click *Create New*.
- Enter a name for the policy.
- Set *Source* set to *cppm-deny*.
- Set *Action* to *DENY*.
- Configure the remaining settings as needed.

The screenshot shows the 'New Policy' configuration window in the FortiGate 60E GUI. The policy is named 'cppm-deny'. The incoming interface is 'port10' and the outgoing interface is 'port9'. The source is 'cppm-deny' and the destination is 'all'. The schedule is 'always' and the service is 'ALL'. The action is set to 'DENY'. The 'Log Violation Traffic' checkbox is checked. The 'Enable this policy' checkbox is also checked.

- f. Click OK.

### To create the firewall policies in the CLI:

```
config firewall address
edit "cppm"
```

```
 set uuid 62a180c0-cb36-51e9-6e70-4a2034d82179
 set type dynamic
 set sub-type clearpass-spt
 set clearpass-spt healthy
 set comment ''
 set visibility enable
 set associated-interface ''
 set color 0
next
edit "cppm-deny"
 set uuid b318e962-cb36-51e9-7a34-74a34cf3bf0b
 set type dynamic
 set sub-type clearpass-spt
 set clearpass-spt infected
 set comment ''
 set visibility enable
 set associated-interface ''
 set color 0
next
end
```

## Verification

Go to *Log & Report > Forward Traffic* to review traffic logs and ensure that traffic is allowed or denied as expected.

To verify that FortiGate addresses are assigned correctly, enter the following CLI command:

```
diagnose firewall dynamic list
List all dynamic addresses:
cppm-deny: ID(141)
 ADDR(10.1.100.188)

cppm: ID(176)
 ADDR(10.1.100.185)
 ADDR(10.1.100.186)
```

## Using wildcard FQDN addresses in firewall policies

You can use wildcard FQDN addresses in firewall policies. IPv4, IPv6, ACL, local, shaping, NAT64, NAT46, and NGFW policy types support wildcard FQDN addresses.

For wildcard FQDN addresses to work, the FortiGate should allow DNS traffic to pass through.

Initially, the wildcard FQDN object is empty and contains no addresses. When the client tries to resolve a FQDN address, the FortiGate will analyze the DNS response. The IP address(es) contained in the answer section of the DNS response will be added to the corresponding wildcard FQDN object. It is therefore necessary to have the DNS session-helpers defined in the `config system session-helper` setting.



Since FortiGate must analyze the DNS response, it does not work with DNS over HTTPS.

---



When the wildcard FQDN gets the resolved IP addresses, FortiOS loads the addresses into the firewall policy for traffic matching.

The FortiGate will keep the IP addresses in the FQDN object table as long as the DNS entry itself has not expired. Once it expires, the IP address is removed from the wildcard FQDN object until another query is made. At any given time, a single wildcard FQDN object may have up to 1000 IP addresses.



The DNS expiry TTL value is set by the authoritative name server for that DNS record. If the TTL for a specific DNS record is very short and you would like to cache the IP address longer, then you can extend it with the CLI. See [To extend the TTL for a DNS record in the CLI: on page 869](#)

For more information, see [FQDN address firewall object type](#).

### To create a wildcard FQDN using the GUI:

1. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
2. Specify a *Name*.
3. For *Type*, select *FQDN*.
4. For *FQDN*, enter a wildcard FQDN address, for example, `*.fortinet.com`.

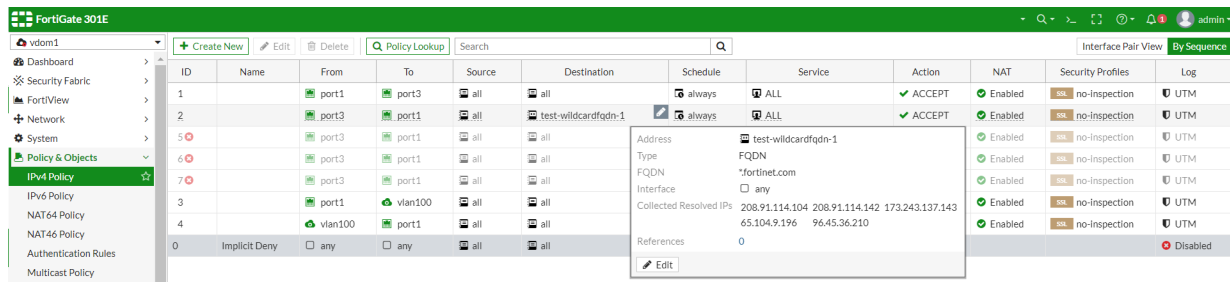
The screenshot shows the FortiGate 301E GUI. On the left, a sidebar lists various configuration categories, with 'Addresses' highlighted in green. The main area is titled 'New Address'. It contains several input fields and checkboxes: 'Name' is 'test-wildcardfqdn-1', 'Type' is 'FQDN', 'FQDN' is '\*.fortinet.com', 'Interface' is 'any', 'Show in Address List' is checked, 'Static Route Configuration' is unchecked, and 'Comments' is 'Write a comment...'. There are also tabs for 'Address', 'IPv6 Address', and 'Multicast Address'.

5. Click *OK*.

### To use a wildcard FQDN in a firewall policy using the GUI:

1. Go to *Policy & Objects > IPv4 Policy* and click *Create New..*
2. For *Destination*, select the wildcard FQDN.
3. Configure the rest of the policy as needed.
4. Click *OK*.

In this example, policy ID 2 uses the wildcard FQDN:



### To create a wildcard FQDN using the CLI:

```
config firewall address
 edit "test-wildcardfqdn-1"
 set uuid 7288ba26-ce92-51e9-04c0-39c707eb4519
 set type fqdn
 set fqdn "*.fortinet.com"
 next
end
```

### To use wildcard FQDN in a firewall policy using the CLI:

```
config firewall policy
 edit 2
 set uuid 2f5ffcc0-cddc-51e9-0642-ab9966b202dd
 set srcintf "port3"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "test-wildcardfqdn-1"
 set action accept
 set schedule "always"
 set service "ALL"
 set auto-asic-offload disable
 set nat enable
 next
end
```

### To use the diagnose command to list resolved IP addresses of wildcard FQDN objects:

```
diagnose firewall fqdn list

List all FQDN:

*.fortinet.com: ID(48) ADDR(96.45.36.159) ADDR(192.168.100.161) ADDR(65.39.139.161)
```

#### Alternatively:

```
diagnose test application dnsproxy 6

worker idx: 0

vfid=0 name=*.fortinet.com ver=IPv4 min_ttl=3266:0, cache_ttl=0 , slot=-1, num=3,
wildcard=1

 96.45.36.159 (ttl=68862:68311:68311) 192.168.100.161 (ttl=3600:3146:3146)
65.39.139.161

(ttl=3600:3481:3481)
```

**To use the diagnose command for firewall policies which use wildcard FQDN:**

```
diagnose firewall iprope list 100004
policy index=2 uuid_idx=46 action=accept
flag (8050108): redir nat master use_src pol_stats
flag2 (4200): no_asic resolve_sso
flag3 (20):
schedule(always)
cos_fwd=255 cos_rev=255
group=00100004 av=00004e20 au=00000000 split=00000000
host=3 chk_client_info=0x0 app_list=0 ips_view=0
misc=0 dd_type=0 dd_mode=0
zone(1): 11 -> zone(1): 9
source(1): 0.0.0.0-255.255.255.255, uuid_idx=0,
destination fqdn or dynamic address (1):
 *.fortinet.com ID(48) uuid_idx=57 ADDR(208.91.114.104) ADDR(208.91.114.142) ADDR
(173.243.137.143) ADDR(65.104.9.196) ADDR(96.45.36.210)
service(1):
 [0:0x0:0/(0,0)->(0,0)] helper:auto
```

**To extend the TTL for a DNS record in the CLI:**

In this the example the set `cache-ttl` value has been extended to 3600 seconds.

```
config firewall address
 edit "fortinet.com"
 set type fqdn
 set fqdn "www.fortinet.com"
 set cache-ttl 3600
 next
end
```

## VIP groups

Virtual IP addresses (VIPs) can be organized into groups. This is useful in scenarios where there are multiple VIPs that are used together in firewall policies. If the VIP group members change, or a group member's settings change (such as the IP address, port, or port mapping type), then those changes are automatically updated in the corresponding firewall policies.

The following table summarizes which VIP types are allowed and not allowed to be members of a VIP group:

Group type	VIP types allowed as members	VIP types not allowed as members
IPv4	<ul style="list-style-type: none"> <li>Static NAT</li> <li>Load balance</li> <li>DNS translation</li> <li>FQDN</li> </ul>	<ul style="list-style-type: none"> <li>Server load balance</li> </ul>
IPv6	<ul style="list-style-type: none"> <li>Static NAT</li> </ul>	<ul style="list-style-type: none"> <li>Server load balance</li> </ul>

Different VIP types can be added to the same group.

**To configure a VIP group in the GUI:**

1. Go to *Policy & Objects > Virtual IPs* and click *Create New > Virtual IP Group*.
2. Set the *Type* to *IPv4*, *IPv6*, *NAT46*, or *NAT64*.
3. Enter a name.
4. Optionally, enter additional information in the *Comments* field.
5. For IPv4 groups, select the *Interface*. Select a specific interface if all of the VIPs are on the same interface; otherwise, select *any*.
6. Click the + in the *Members* field and select the members to add to the group.
7. Click *OK*.

**To configure an IPv4 VIP group in the CLI:**

```
config firewall vipgrp
 edit <name>
 set interface <name>
 set member <vip1> <vip2> ...
 next
end
```

**To configure an IPv6 VIP group in the CLI:**

```
config firewall vipgrp6
 edit <name>
 set member <vip1> <vip2> ...
 next
end
```

## Traffic shaping

QoS (quality of service) is the capability to adjust quality aspects of your overall network traffic, including techniques such as priority-based queuing and traffic policing. Because bandwidth is finite and some types of traffic are slow, jitter or packet loss sensitive, bandwidth intensive, or critical for operations, QoS is a useful tool to optimize the performance of various applications in your network. QoS is especially important for managing voice and streaming multimedia traffic because these types of traffic can rapidly consume bandwidth and are sensitive to latency. You can implement QoS on FortiGate devices using the following techniques:

Technique	Description
Traffic policing	The FortiGate drops packets that do not conform to the configured bandwidth limitations.  Note that excessive traffic policing can degrade network performance rather than improve it.
Traffic shaping	The FortiGate ensures that traffic consumes bandwidth at least at the guaranteed rate by assigning a greater priority queue to the traffic if the guaranteed rate is not being met.

Technique	Description
	The FortiGate ensures that traffic does not consume more than the maximum configured bandwidth. Traffic that exceeds the maximum rate is subject to traffic policing.
Queuing	The FortiGate transmits packets in the order of their assigned priority queue for that physical interface. All traffic in a higher priority traffic queue must be completely transmitted before traffic in lower priority queues is transmitted.

When determining how to configure QoS, it is helpful to know when a FortiGate uses each technique in the overall traffic processing flow and the considerations for each technique. After the FortiGate accepts packets, it classifies the traffic and may apply traffic policing at additional points during traffic processing. The FortiGate may also apply QoS techniques, such as prioritization and traffic shaping. Traffic shaping consists of both traffic policing to enforce bandwidth limits and adjusting priority queues to help packets achieve the guaranteed rate.

Traffic shaping accuracy is optimal for security policies without a protection profile where no FortiGate content inspection is processed.



You can enable traffic shaping in *System > Feature Visibility* under the *Additional Features* section.

The following topics provide information about configuring traffic shaping policies:

- [Determining your QoS requirements on page 871](#)
- [Packet rates on page 873](#)
- [Interface bandwidth limit on page 874](#)
- [Changing traffic shaper bandwidth unit of measurement on page 875](#)
- [Shared traffic shaper on page 876](#)
- [Per-IP traffic shaper on page 880](#)
- [Type of Service-based prioritization and policy-based traffic shaping on page 883](#)
- [Interface-based traffic shaping profile on page 886](#)
- [Classifying traffic by source interface on page 894](#)
- [Configuring traffic class IDs on page 895](#)
- [Traffic shaping schedules on page 897](#)
- [QoS assignment and rate limiting for quarantined VLANs on page 899](#)
- [Weighted random early detection queuing on page 900](#)

## Determining your QoS requirements

Before implementing QoS, you should identify the types of traffic that:

- Are important to your organization
- Use high amounts of bandwidth
- Are sensitive to latency or packet loss

Discovering the needs and relative importance of each traffic type on your network will help you design an appropriate overall approach, including how you configure each available QoS component technique. Some organizations discover

they only need to configure bandwidth limits for some services. Other organizations determine they need to fully configure interface and security policy bandwidth limits for all services, and prioritize the queuing of critical services relative to traffic rate.

For example, your organization wants to guarantee sufficient bandwidth for revenue-producing e-commerce traffic. You need to ensure that customers complete transactions and do not experience service delays. At the same time, you need to ensure low latency for voice over IP (VoIP) traffic that sales and customer support teams use, while traffic latency and bursts may be less critical to the success of other network applications, such as long term, resumable file transfers.

## Best practices

The following list includes recommendations and considerations when configuring QoS in your network:

- Ensure maximum bandwidth limits at the source interface and security policy are not too low. This can cause the FortiGate to discard an excessive number of packets.
- Consider the ratios of how packets are distributed between the available queues, and which queues are used by which types of services. Assigning most packets to the same priority queue can reduce the effects of configuring prioritization. Assigning a lot of high bandwidth services to high priority queues may take too much bandwidth away from lower priority queues and cause increased or indefinite latency. For example, you may want to prioritize a latency-sensitive service, such as SIP, over a bandwidth-intensive service, such as FTP. Also consider that bandwidth guarantees can affect queue distribution, and assign packets to queue 0 instead of their regular queue in high-volume situations.
- Decide whether or not to guarantee bandwidth because it causes the FortiGate to assign packets to queue 0 if the guaranteed packet rate is not being met. When you compare queuing behavior for low and high bandwidth situations, this means the effect of prioritization only becomes visible as traffic volumes rise and exceed their guarantees. Because of this, you might want only some services to use bandwidth guarantees. This way, you can avoid the possibility that all traffic uses the same queue in high-volume situations, which negates the effects of configuring prioritization.
- Configure prioritization for all through traffic by either ToS (type of service)-based priority or security policy priority, not both, to simplify analysis and troubleshooting. Traffic subject to both ToS-based and security policy priorities use a combined priority from both parts of the configuration. Traffic subject to only one of the prioritization methods will use only that priority. If you configure both methods, or if you configure either method for only a subset of traffic, packets that apply to the combined configuration may receive a lower priority queue than packets that apply to only one of the priority methods, as well as packets that do not apply to the configured prioritization. For example, if both the ToS-based priority and security policy priority dictate that a packet should receive a medium priority, in the absence of bandwidth guarantees, a packet will use queue 3. If only ToS-based priority is configured, the packet will use queue 1. If only security policy priority is configured, the packet will use queue 2. If no prioritization is configured, the packet will use queue 0.
  - Because you can configure QoS using a combination of security policies and ToS-based priorities, and to distribute traffic over the six possible queues for each physical interface, the results of those configurations can be more difficult to analyze because of their complexity. In those cases, prioritization behavior can vary by several factors, including: traffic volume, ToS or differentiated services (DiffServ) markings, and correlation of session to a security policy.



The FortiGate does not prioritize traffic based on the differentiated services code point (DSCP) marking configured in the security policy. However, ToS-based prioritization can be used for ingress traffic.

---

- Use the UDP protocol to obtain more accurate testing results. Packets that are discarded by traffic shapers impact flow-control mechanisms, such as TCP.
- Do not oversubscribe outbound throughput. For example,  $\text{sum}[\text{guaranteed bandwidth}] < \text{outbandwidth}$ . For accurate bandwidth calculations, you must set the outbandwidth parameter on interfaces.

## Packet rates

The formula for packet rates specified for maximum bandwidth or guaranteed bandwidth is:

rate = amount / time

where rate is in Kbps

Burst size cannot exceed the configured maximum bandwidth. The FortiGate drops packets that exceed the configured maximum bandwidth. Packets deduct from the amount of bandwidth available to subsequent packets, and available bandwidth regenerates at a fixed rate. As a result, the available bandwidth for a packet may be less than the configured rate, down to a minimum of 0 Kbps.

Alternatively, rate calculation and behavior can be described using the token bucket metaphor. A traffic flow has an associated bucket, which represents burst size bounds and is the size of the configured bandwidth limit. The bucket receives tokens, which represent available bandwidth at the fixed configured rate. As time passes, tokens are added to the bucket up to capacity, and excess tokens are discarded. When a packet arrives at the FortiGate, the packet must deduct bandwidth tokens from the bucket equal to its size in order to leave the FortiGate. If there are not enough tokens, the packet cannot leave the FortiGate and is dropped.

Bursts are not redistributed over a longer interval, so bursts are propagated rather than smoothed. However, peak size is limited. The maximum burst size is the capacity of the bucket, which is the configured bandwidth limit. The actual size varies depending on the current number of tokens in the bucket, which may be less than the capacity of the bucket due to deductions made by previous packets and the fixed rate at which tokens accumulate. A depleted bucket refills at the rate of the configured bandwidth limit. Bursts cannot borrow tokens from other time intervals.

By limiting traffic peaks and token regeneration, the available bandwidth may be less than the capacity of the bucket, but the limit of the total amount per time interval is ensured. Total bandwidth use during each interval of one second is, at most, the integral of the configured rate.

## Rate discrepancy

You may observe that external clients, such as FTP or BitTorrent, initially report rates between the maximum bandwidth and twice the amount of the maximum bandwidth depending on the size of their initial burst. For example, when a connection is initiated following a period of no network activity. The apparent discrepancy in rates is caused by a difference in perspective when delimiting time intervals. A burst from the client may initially consume all tokens in the bucket, and before the end of one second as the bucket regenerates, is allowed to consume almost another bucket worth of bandwidth. From the perspective of the client, this equals one time interval. However, from the perspective of the FortiGate, the bucket cannot accumulate tokens when it is full. Therefore, the time interval for token regeneration begins after the initial burst and does not contain the burst. These different points of reference result in an initial discrepancy equal to the size of the burst. The client's rate contains it, but the FortiGate's rate does not. However, if the connection is sustained to its limit and time progresses over an increasing number of intervals, this discrepancy decreases in importance relative to the bandwidth total. The client reported rate will eventually approach the configured rate limit for the FortiGate.

## Example

The maximum bandwidth is 50 Kbps, there has been no network activity for one or more seconds, and the bucket is full. A burst from an FTP client immediately consumes 50 kilobits. Because the bucket completely regenerates over one second, by the time another second elapses from the initial burst, traffic can consume another 49.999 kilobits, for a total of 99.999 kilobits between the two points in time. From the vantage point of an external FTP client regulated by this bandwidth limit, it initially appears that the bandwidth limit is 99.999 Kbps. This is almost twice the configured limit of 50 Kbps. However, bucket capacity only regenerates at the configured rate of 50 Kbps, and the connection can only

consume a maximum of 50 kilobits during each subsequent second. The result is that as bandwidth consumption is averaged over an increasing number of time intervals, each of which are limited to 50 Kbps, the effect of the first interval's doubled bandwidth size diminishes proportionately, and the client's reported rate eventually approaches the configured rate limit. The following table shows the effects of a 50 Kbps limit on client reported rates:

Total size transferred (kilobits)	Time (seconds)	Rate reported by client (Kbps)
99.999 (50 + 49.999)	1	99.999
149.999	2	74.999
199.999	3	66.666
249.999	4	62.499
299.999	5	59.998
349.999	6	58.333

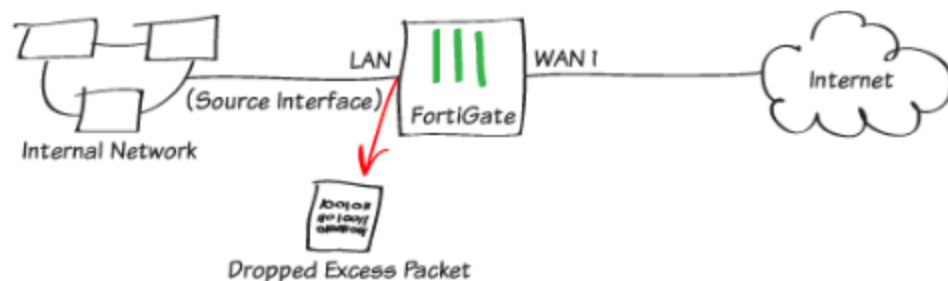
Guaranteed bandwidth can also be described using a token bucket metaphor. However, because this feature attempts to achieve or exceed a rate rather than limit it, the FortiGate does not discard non-conforming packets, as it does for maximum bandwidth. Instead, when the flow does not achieve the rate, the FortiGate increases the packet priority queue, in an effort to increase the rate.

Guaranteed and maximum bandwidth rates apply to the bidirectional total for all sessions controlled by the security policy. For example, an FTP connection may entail two separate connections for the data and control portion of the session. Some packets may be reply traffic rather than initiating traffic. All packets for both connections are counted when calculating the packet rate for comparison with the guaranteed and maximum bandwidth rate.

## Interface bandwidth limit

You can limit interface bandwidth for arriving and departing traffic. In some cases, the traffic received on an interfaces could exceed the maximum bandwidth limit defined in the security policy. Rather than waste processing power on packets that will get dropped later in the process, you can configure FortiGate to preemptively drop excess packets when they're received at the source interface. A similar command is available to the outgoing interface.

The following diagram shows how excess packets going from LAN to WAN1 can be intercepted and dropped at the source interface.





**To configure an interface bandwidth limit in the GUI:**

1. Go to *Network > Interfaces*.
2. Edit port1.
3. In the *Traffic Shaping* section set the following options:
  - a. Enable *Inbound Bandwidth* and enter 200.  
The default bandwidth unit is kbps.
  - b. Enable *Outbound Bandwidth* and enter 400.  
The default bandwidth unit is kbps.
4. Click *OK*.

**To configure an interface bandwidth limit in the CLI:**

1. On the FortiGate, configure the interface bandwidth limit:

```
config system interface
 edit "port1"

 set inboundwidth 200
 set outboundwidth 400

 next
end
```

## Changing traffic shaper bandwidth unit of measurement

Bandwidth speeds are measured in kilobits per second (Kbps), and bytes that are sent and received are measured in megabytes (MB). In some cases, this can cause confusion depending on whether your ISP uses kilobits per second (Kbps), kilobytes per second (KBps), megabits per second (Mbps), or gigabits per second (Gbps).

You can change the unit of measurement for traffic shapers in the CLI.

**To change the bandwidth unit of measurement for a shared traffic shaper:**

```
config firewall shaper traffic-shaper
 edit <traffic_shaper_name>
 set bandwidth-unit {kbps | mbps | gbps}
 next
end
```

**To change the bandwidth unit of measurement for a per-IP traffic shaper:**

```
config firewall shaper per-ip-shaper
 edit <traffic_shaper_name>
 set bandwidth-unit {kbps | mbps | gbps}
 next
end
```

## Shared traffic shaper

Shared traffic shaper is used in a firewall shaping policy to indicate the priority and guaranteed and maximum bandwidth for a specified type of traffic use.

The maximum bandwidth indicates the largest amount of traffic allowed when using the policy. You can set the maximum bandwidth to a value between 1 and 16776000 Kbps. The GUI displays an error if any value outside this range is used. If you want to allow unlimited bandwidth, use the CLI to enter a value of 0.

The guaranteed bandwidth ensures that there is a consistent reserved bandwidth available. When setting the guaranteed bandwidth, ensure that the value is significantly less than the interface's bandwidth capacity. Otherwise, the interface will allow very little or no other traffic to pass through, potentially causing unwanted latency.

In a shared traffic shaper, the administrator can prioritize certain traffic as high, medium, or low. FortiOS provides bandwidth to low priority connections only when high priority connections do not need the bandwidth. For example, you should assign a high traffic priority to a policy for connecting a secure web server that needs to support e-commerce traffic. You should assign less important services a low priority.

When you configure a shared traffic shaper, you can apply bandwidth shaping per policy or for all policies. By default, a shared traffic shaper applies traffic shaping evenly to all policies that use the shared traffic shaper.

When configuring a per-policy traffic shaper, FortiOS applies the traffic shaping rules defined for each security policy individually. For example, if a per-policy traffic shaper is configured with a maximum bandwidth of 1000 Kbps, any security policies that have that traffic shaper enabled get 1000 Kbps of bandwidth each.

If a traffic shaper for all policies is configured with a maximum bandwidth of 1000 Kbps, all policies share the 1000 Kbps on a first-come, first-served basis.

The configuration is as follows:

```
config firewall shaper traffic-shaper
 edit "traffic_shaper_name"
 set per-policy enable
 next
end
```

The shared traffic shaper selected in the traffic shaping policy affects traffic in the direction defined in the policy. For example, if the source port is LAN and the destination is WAN1, the traffic shaping affects the flow in this direction only, affecting the outbound traffic's upload speed. You can define the traffic shaper for the policy in the opposite direction (reverse shaper) to affect the inbound traffic's download speed. In this example, that would be from WAN1 to LAN.

Only traffic through forward traffic shapers will be included in FortiView; reverse and per-IP shapers are not included.

The following example shows how to apply different speeds to different types of service. The example configures two shared traffic shapers to use in two firewall shaping policies. One policy guarantees a speed of 10 Mbps for VoIP traffic. The other policy guarantees a speed of 1 Mbps for other traffic. In the example, FortiOS communicates with a PC using port10 and the Internet using port9.

### To configure shared traffic shapers in the GUI:

1. Create a firewall policy:
  - a. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
  - b. Set the *Name* to *Internet Access*.
  - c. Set the *Incoming Interface* to *port10*.
  - d. Set the *Outgoing Interface* to *port9*.
  - e. Set the *Source* and *Destination* to *all*.

- f. Set the *Schedule* to *always*.
  - g. Set the *Service* to *ALL*.
  - h. Click *OK*.
2. Create the shared traffic shapers:
- a. Go to *Policy & Objects > Traffic Shapers* and click *Create New*.
  - b. Set the *Name* to *10Mbps*. This shaper is for VoIP traffic.
  - c. Set the *Traffic Priority* to *High*.
  - d. Enable *Max Bandwidth* and enter *20000*.
  - e. Enable *Guaranteed Bandwidth* and enter *10000*.

New Traffic Shaper

Type: **Shared** Per IP Shaper

Name: 10Mbps

Quality of Service

Traffic priority: High

Bandwidth unit: kbps

Maximum bandwidth: ☒ 20000 kbps

Guaranteed bandwidth: ☒ 10000 kbps

DSCP: ☐

OK Cancel

- f. Click *OK*.
  - g. Repeat the above steps to create another traffic shaper named *1Mbps* with the *Traffic Priority* set to *Low*, the *Max Bandwidth* set to *10000*, and the *Guaranteed Bandwidth* set to *1000*.
3. Create a firewall shaping policy:
- a. Go to *Policy & Objects > Traffic Shaping Policy* and click *Create New*.
  - b. Set the *Name* to *VoIP\_10Mbps\_High*. This policy is for VoIP traffic.
  - c. Set the *Source* and *Destination* to *all*.
  - d. Set the *Service* to all VoIP services.
  - e. Set the *Outgoing Interface* to *port9*.
  - f. Enable *Shared shaper* and select *10Mbps*.
  - g. Enable *Reverse shaper* and select *10Mbps*.
  - h. Click *OK*.
  - i. Repeat the above steps to create another firewall shaping policy named *Other\_1Mbps\_Low* for other traffic, with the *Source* and *Destination* set to *all*, *Service* set to *ALL*, *Outgoing Interface* set to *port9*, and *Shared shaper* and *Reverse shaper* set to *1Mbps*.

### To configure shared traffic shapers in the CLI:

1. Create a firewall policy:

```
config firewall policy
 edit 1
 set name "Internet Access"
 set srcintf "port10"
 set dstintf "port9"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set fsso disable
 set nat enable
```

```
 next
end
```

**2. Create the shared traffic shapers:**

```
config firewall shaper traffic-shaper
 edit "10Mbps"
 set guaranteed-bandwidth 10000
 set maximum-bandwidth 20000
 next
 edit "1Mbps"
 set guaranteed-bandwidth 1000
 set maximum-bandwidth 10000
 set priority low
 next
end
```

**3. Create a firewall shaping policy:**

```
config firewall shaping-policy
 edit 1
 set name "VOIP_10Mbps_High"
 set service "H323" "IRC" "MS-SQL" "MYSQL" "RTSP" "SCCP" "SIP" "SIP-MSNmessenger"
 set dstintf "port9"
 set traffic-shaper "10Mbps"
 set traffic-shaper-reverse "10Mbps"
 set srcaddr "all"
 set dstaddr "all"
 next
 edit 2
 set name "Other_1Mbps_Low"
 set service "ALL"
 set dstintf "port9"
 set traffic-shaper "1Mbps"
 set traffic-shaper-reverse "1Mbps"
 set srcaddr "all"
 set dstaddr "all"
 next
end
```

**To troubleshoot shared traffic shapers:**

1. To check if specific traffic is attached to the correct traffic shaper, run the `diagnose firewall iprope list 100015` command. The example output shows the traffic attached to the 10Mbps and 1Mbps shapers:

```
diagnose firewall iprope list 100015
```

```
policy index=1 uuid_idx=0 action=accept
flag (0):
shapers: orig=10Mbps(2/1280000/2560000)
cos_fwd=0 cos_rev=0
group=00100015 av=00000000 au=00000000 split=00000000
host=4 chk_client_info=0x0 app_list=0 ips_view=0
misc=0 dd_type=0 dd_mode=0
zone(1): 0 -> zone(1): 38
source(1): 0.0.0.0-255.255.255.255, uuid_idx=0,
dest(1): 0.0.0.0-255.255.255.255, uuid_idx=0,
service(15):
 [6:0x0:0/(1,65535)->(1720,1720)] helper:auto
 [6:0x0:0/(1,65535)->(1503,1503)] helper:auto
 [17:0x0:0/(1,65535)->(1719,1719)] helper:auto
```

```
[6:0x0:0/(1,65535)->(6660,6669)] helper:auto
[6:0x0:0/(1,65535)->(1433,1433)] helper:auto
[6:0x0:0/(1,65535)->(1434,1434)] helper:auto
[6:0x0:0/(1,65535)->(3306,3306)] helper:auto
[6:0x0:0/(1,65535)->(554,554)] helper:auto
[6:0x0:0/(1,65535)->(7070,7070)] helper:auto
[6:0x0:0/(1,65535)->(8554,8554)] helper:auto
[17:0x0:0/(1,65535)->(554,554)] helper:auto
[6:0x0:0/(1,65535)->(2000,2000)] helper:auto
[6:0x0:0/(1,65535)->(5060,5060)] helper:auto
[17:0x0:0/(1,65535)->(5060,5060)] helper:auto
[6:0x0:0/(1,65535)->(1863,1863)] helper:auto
```

```
policy index=2 uuid_idx=0 action=accept
flag (0):
shapers: orig=1Mbps(4/128000/1280000)
cos_fwd=0 cos_rev=0
group=00100015 av=00000000 au=00000000 split=00000000
host=4 chk_client_info=0x0 app_list=0 ips_view=0
misc=0 dd_type=0 dd_mode=0
zone(1): 0 -> zone(1): 38
source(1): 0.0.0.0-255.255.255.255, uuid_idx=0,
dest(1): 0.0.0.0-255.255.255.255, uuid_idx=0,
service(1):
[0:0x0:0/(0,0)->(0,0)] helper:auto
```

2. To check if the correct traffic shaper is applied to the session, run the `diagnose sys session list` command. The example output shows that the 1Mbps shaper is applied to the session:

```
diagnose sys session list
session info: proto=6 proto_state=01 duration=11 expire=3599 timeout=3600 flags=00000000
sockflag=00000000 sockport=0 av_idx=0 use=5
origin-shaper=1Mbps prio=4 guarantee 128000Bps max 1280000Bps traffic 1050Bps drops 0B
reply-shaper=
per_ip_shaper=
class_id=0 shaping_policy_id=2 ha_id=0 policy_dir=0 tunnel=/ helper=ftp vlan_cos=0/255
state=may_dirty npu npd os mif route_preserve
statistic(bytes/packets/allow_err): org=868/15/1 reply=752/10/1 tuples=2
tx speed(Bps/kbps): 76/0 rx speed(Bps/kbps): 66/0
orgin->sink: org pre->post, reply pre->post dev=39->38/38->39 gwy=172.16.200.55/0.0.0.0
hook=post dir=org act=snat 10.1.100.11:58241->172.16.200.55:21(172.16.200.1:58241)
hook=pre dir=reply act=dnat 172.16.200.55:21->172.16.200.1:58241(10.1.100.11:58241)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=4
serial=0003255f tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x100000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0,
vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason: offload-denied helper
total session 1
```

3. To check statuses of shared traffic shapers, run the `diagnose firewall shaper traffic-shaper list` command. The output should resemble the following:

```
diagnose firewall shaper traffic-shaper list

name 10Mbps
```

```
maximum-bandwidth 2500 KB/sec
guaranteed-bandwidth 1250 KB/sec
current-bandwidth 0 B/sec
priority 2
tos ff
packets dropped 0
bytes dropped 0

name 1Mbps
maximum-bandwidth 1250 KB/sec
guaranteed-bandwidth 125 KB/sec
current-bandwidth 0 B/sec
priority 4
tos ff
packets dropped 0
bytes dropped 0
```

## Per-IP traffic shaper

With per-IP traffic shaping, you can limit each IP address's behavior to avoid a situation where one user uses all of the available bandwidth. In addition to controlling the maximum bandwidth used per IP address, you can also define the maximum number of concurrent sessions for an IP address. For example, if you apply a per-IP shaper of 1 Mbps to your entire network, FortiOS allocates each user/IP address 1 Mbps of bandwidth. Even if the network consists of a single user, FortiOS allocates them 1 Mbps. If there are ten users, each user gets 1 Mbps of bandwidth, totaling 10 Mbps of outgoing traffic.

For shared shapers, all users share the set guaranteed and maximum bandwidths. For example, if you set a shared shaper for all PCs using an FTP service to 10 Mbps, all users uploading to the FTP server share the 10 Mbps.

Shared shapers affect upload speed. If you want to limit the download speed from the FTP server in the example, you must configure the shared shaper as a reverse shaper. Per-IP shapers apply the speed limit on both upload and download operations. Only traffic through forward traffic shapers will be included in FortiView; reverse and per-IP shapers are not included.

The following example shows how to apply a per-IP shaper to a traffic shaping policy. This shaper assigns each user a maximum bandwidth of 1 Mbps and allows each user to have a maximum of ten concurrent connections to the FTP server. In the example, FortiOS communicates with users using port10 and the FTP server using port9.

### To configure a per-IP traffic shaper in the GUI:

1. Create a firewall policy:
  - a. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
  - b. Set the *Name* to *FTP Access*.
  - c. Set the *Incoming Interface* to *port10*.
  - d. Set the *Outgoing Interface* to *port9*.
  - e. Set the *Source* to *all*.
  - f. Set the *Destination* to *FTP\_Server*.
  - g. Set the *Schedule* to *always*.
  - h. Set the *Service* to *ALL*.
  - i. Click *OK*.

## 2. Create the per-IP traffic shaper:

- a. Go to *Policy & Objects > Traffic Shapers* and click *Create New*.
- b. Set *Type* to *Per IP Shaper*.
- c. Set the *Name* to *FTP\_Max\_1M*. This shaper is for VoIP traffic.
- d. Enable *Max Bandwidth* and enter *1000*.
- e. Enable *Max Concurrent Connections* and enter *10*. This means that each user can have up to ten concurrent connections to the FTP server.

- f. Click *OK*.

## 3. Create a firewall shaping policy:

- a. Go to *Policy & Objects > Traffic Shaping Policy* and click *Create New*.
- b. Set the *Name* to *FTP speed 1M*.
- c. Set the *Source* to the addresses and users that require access to the FTP server.
- d. Set the *Destination* to *FTP\_Server*.
- e. Set the *Service* to *ALL*.
- f. Set the *Outgoing Interface* to *port9*.
- g. Enable *Per-IP shaper* and select *FTP\_Max\_1M*.
- h. Click *OK*.

## To configure a per-IP traffic shaper in the CLI:

### 1. Create a firewall policy:

```
config firewall policy
 edit 1
 set name "FTP Access"
 set srcintf "port10"
 set dstintf "port9"
 set srcaddr "all"
 set dstaddr "FTP_Server"
 set action accept
 set schedule "always"
 set service "ALL"
 set fsso disable
 set nat enable
 next
end
```

### 2. Create the per-IP traffic shaper:

```
config firewall shaper per-ip-shaper
 edit "FTP_Max_1M"
 set max-bandwidth 1000
 set max-concurrent-session 10
 next
```

```
end
```

### 3. Create a firewall shaping policy:

```
config firewall shaping-policy
 edit 1
 set name "FTP speed 1M"
 set service "ALL"
 set dstintf "port9"
 set per-ip-shaper "FTP_Max_1M"
 set srcaddr "PC1" "WinPC" "PC2"
 set dstaddr "FTP_Server"
 next
end
```

## To troubleshoot per-IP traffic shapers:

1. To check if specific traffic is attached to the correct traffic shaper, run the `diagnose firewall iprope list 100015` command. The example output shows the traffic attached to the `FTP_Max_1M` shaper:

```
diagnose firewall iprope list 100015
```

```
policy index=3 uuid_idx=0 action=accept
flag (0):
shapers: per-ip=FTP_Max_1M
cos_fwd=0 cos_rev=0
group=00100015 av=00000000 au=00000000 split=00000000
host=2 chk_client_info=0x0 app_list=0 ips_view=0
misc=0 dd_type=0 dd_mode=0
zone(1): 0 -> zone(1): 38
source(3): 10.1.100.11-10.1.100.11, uuid_idx=30, 10.1.100.143-10.1.100.143, uuid_idx=32,
 10.1.100.22-10.1.100.22, uuid_idx=31,
dest(1): 172.16.200.55-172.16.200.55, uuid_idx=89,
service(1):
[0:0x0:0/(0,65535)->(0,65535)] helper:auto
```

2. To check if the correct traffic shaper is applied to the session, run the `diagnose sys session list` command. The example output shows that the `FTP_Max_1M` shaper is applied to the session:

```
diagnose sys session list
session info: proto=6 proto_state=01 duration=36 expire=3567 timeout=3600 flags=00000000
 sockflag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=FTP_Max_1M
class_id=0 shaping_policy_id=3 ha_id=0 policy_dir=0 tunnel=/ helper=ftp vlan_cos=0/255
state=may_dirty per_ip npu npd mif route_preserve
statistic(bytes/packets/allow_err): org=506/9/1 reply=416/6/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=39->38/38->39 gwy=172.16.200.55/0.0.0.0
hook=post dir=org act=snat 10.1.100.11:58275->172.16.200.55:21(172.16.200.1:58275)
hook=pre dir=reply act=dnat 172.16.200.55:21->172.16.200.1:58275(10.1.100.11:58275)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=2
serial=0000211a tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x100000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0,
 vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
```



```
no_ofld_reason: offload-denied helper
```

3. To check statuses of per-IP traffic shapers, run the `diagnose firewall shaper per-ip-shaper list` command. The output should resemble the following:

```
diagnose firewall shaper per-ip-shaper list

name FTP_Max_1M
maximum-bandwidth 125 KB/sec
maximum-concurrent-session 10
tos ff/ff
packets dropped 0
bytes dropped 0
addr=10.1.100.11 status: bps=0 ses=3
```

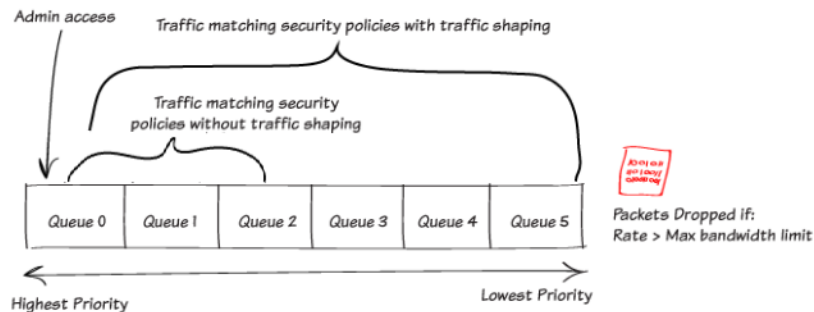
## Type of Service-based prioritization and policy-based traffic shaping

### Priority queues

After packet acceptance, FortiOS classifies traffic and may apply Quality of Service (QoS) techniques, such as prioritization and traffic shaping. Traffic shaping consists of a mixture of traffic policing to enforce bandwidth limits and priority queue adjustment to assist packets in achieving the guaranteed rate.

If you have configured prioritization, FortiOS prioritizes egressing packets by distributing them among first in first out (FIFO) queues associated with each possible priority number. Each physical interface has six priority queues. Virtual interfaces use the priority queues of the physical interface that they are bound to.

The physical interface's six queues are queue 0 to 5, where queue 0 is the highest priority queue. You might observe that your traffic uses only a subset of those six queues. For example, some traffic may always use a certain queue number. Queuing may also vary by the packet rate or mixture of services. Some queue numbers may only be used by through traffic for which you have configured traffic shaping in the security policy that applies to that traffic session.



- Administrative access traffic always uses queue 0.
- Traffic matching firewall policies without traffic shaping may use queue 0, 1, or 2. The queue is selected based on the priority value you have configured for packets with that ToS bit value, if you have configured ToS-based priorities.
- Traffic matching firewall shaping policies with traffic shaping enabled can use any queue. The queue is selected based on whether the packet rate is currently below the guaranteed bandwidth (queue 0), or above the guaranteed bandwidth. Packets at rates greater than the maximum bandwidth limit are dropped.

### Priority types

Packets can be assigned a priority in one of three types:

- On entering ingress – for packets flowing through the firewall.
- Upon generation – for packets generated by the firewall (including packets generated due to AV proxying).
- On passing through a firewall policy – for packets passing through a firewall policy (firewall shaping policy) that has a traffic shaper defined.

## ToS priority

The first and second types, ingress priority and priority for generated packets, are controlled by two different CLI settings:

```
config system global
 set traffic-priority-level {high | medium | low}
end
config system tos-based-priority
 edit 1
 set tos [0-15] <---- type of service bit in the IP datagram header with a value
between 0 and 15
 set priority (high | medium | low) <---- priority of this type of service
 next
end
```

Each priority level is mapped to a value as follows:

ToS priority	Value
High	0
Medium	1
Low	2



ToS-based traffic prioritization cannot be used to apply bandwidth limits and guarantees, but can be used to prioritize traffic at per-packet levels.

## Example

In the following example configuration, packets with ToS bit values of 10 are prioritized as medium and packets with ToS bit values of 20 are prioritized as high. All the other traffic is prioritized as low.

```
config system global
 set traffic-priority-level low
end
config system tos-based-priority
 edit 1
 set tos 10
 set priority medium
 next
 edit 2
 set tos 20
 set priority high
 next
end
```

## Firewall shaping policy priority

You can enable traffic shaping in a firewall shaping policy. In the shared traffic shaper, you can set the firewall priority to high, medium, or low:

```
config firewall shaper traffic-shaper
 edit 1
 set priority {high | medium | low}
 next
end
```

As the priority in a traffic shaper is set to high by default, you must set some traffic at a lower priority to see results. Each priority level is mapped to a value as follows:

Firewall policy priority	Value
High (default)	1
Medium	2
Low	3

## Combination of two priority types

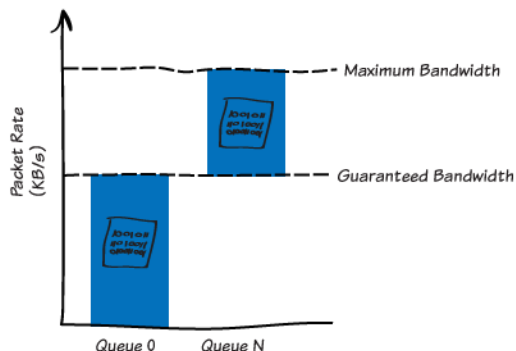
To combine the two priority types, the global or ingress ToS-based priority value is combined with the firewall policy priority value:

$$\text{ToS priority (0, 1, 2)} + \text{policy priority (1, 2, 3)} = \text{total priority (queue number)}$$

Consider the following scenarios:

- If the current packet rate is less than the guaranteed bandwidth, packets use priority queue 0. Packet priority is 0.
- If the current packet rate exceeds the maximum bandwidth, excess packets are dropped.
- If the current packet rate is greater than the guaranteed bandwidth but less than the maximum bandwidth, FortiOS assigns a priority queue by adding the ToS-based priority and the firewall priority.

For example, if you have enabled traffic shaping in the security policy and the security policy's traffic priority is low (value 3), and the priority normally applied to packets with that ToS bit is medium (value 1), the packets have a total packet priority of 4, and use priority queue 4.



## Interface-based traffic shaping profile

A traffic shaping policy can be used for interface-based traffic shaping by organizing traffic into 30 class IDs. The shaping profile defines the percentage of the interface bandwidth that is allocated to each class. Each traffic class ID is shaped to the assigned speed according to the outgoing bandwidth limit configured to the interface.

### Traffic classification

A shaping policy classifies traffic and organizes it into different class IDs, based on matching criteria. For traffic matching a criteria, you can choose to put it into 30 different shaping classes, identified by class ID 2 to 31.

You must select an outgoing interface for the traffic. The shaping policy is only applied when the traffic goes to one of the selected outgoing interfaces.

Criterion	Description
<b>Source</b>	<ul style="list-style-type: none"> <li>Address: match the source address of the traffic to the selected address or address group.</li> <li>User: use the user credentials of the traffic to match the selected user or user group. At least one address, address group, or internet service must also be selected.</li> <li>Internet service: match the traffic to the selected internet service. Internet services cannot be used if addresses or address or groups are used.</li> </ul>
<b>Destination</b>	<ul style="list-style-type: none"> <li>Address: match the destination address of the traffic to the selected address or address group.</li> <li>Internet service: match the traffic to the selected internet service. Internet services cannot be used if addresses or address or groups are used.</li> </ul>
<b>Schedule</b>	Match the current date and time to the selected schedule. You can select a one-time schedule, recurring schedule, or schedule group. This setting is optional.
<b>Service</b>	Match the service of the traffic to the selected service or service group.
<b>Application</b>	<p>Match the application of the traffic to the selected application, application category, or application group.</p> <p>Application control must be enabled in the related firewall policy to know the application of the traffic. See <a href="#">Application control on page 1021</a> for more information.</p>
<b>URL category</b>	<p>Match the URL of the traffic to the selected URL category.</p> <p>Web filter must be enabled in the related firewall policy to know the URL of the traffic. See <a href="#">Web filter on page 947</a> for more information.</p>



When multiple items are selected in one criterion, it is considered a match when traffic matches any one of them.

## Traffic prioritization

Shaping profiles define how different shaping classes of traffic are prioritized. For each class, you can define three prioritization strategies: guaranteed bandwidth, maximum bandwidth, and priority.

For each shaping profile, a default shaping class must be defined. Traffic is prioritized based on the default shaping group in the following two circumstances:

- All traffic to the outgoing interface that does not match to any shaping policy
- Traffic with a shaping group that is not defined in a shaping profile

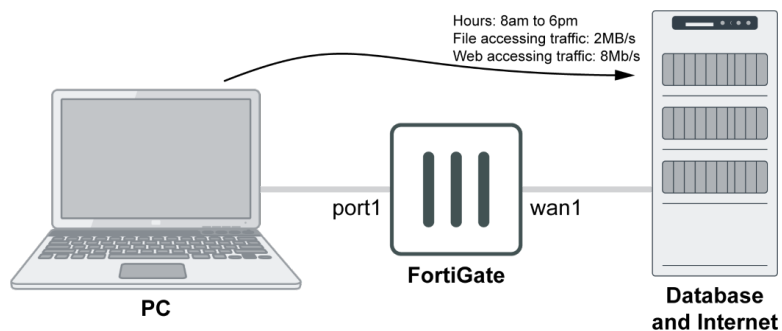
Prioritization strategy	Description
<b>Guaranteed bandwidth</b>	The percentage of the link speed that is reserved for the shaping group. The total guaranteed bandwidth for all shaping groups cannot exceed 100%.
<b>Maximum bandwidth</b>	The maximum percentage of the link speed that the shaping group can use.
<b>Priority</b>	The shaping class priority: top, critical, high, medium, or low. When groups are competing for bandwidth on the interface, the group with the higher priority wins.

## Applying a shaping profile to an interface

Traffic shaping is accomplished by configuring the outgoing bandwidth and outgoing shaping profile on an interface. The shaping profile uses the outgoing bandwidth of the interface as the maximum link speed, and it only works when the outgoing bandwidth is configured.

This example shows how to apply interface-based traffic shaping to web and file accessing traffic according to a schedule:

- The link speed of the wan1 interface is 10 Mb/s.
- File access can use up to 2 Mb/s from 8:00 AM to 6:00 PM.
- Web access can use 8 Mb/s from 8:00 AM to 6:00 PM.



## Putting the traffic into shaping classes

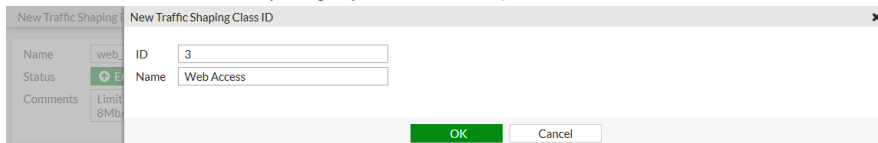
To create a recurring schedule in the GUI:

1. Go to *Policy & Objects > Schedules*.
2. Click *Create New > Schedule*.

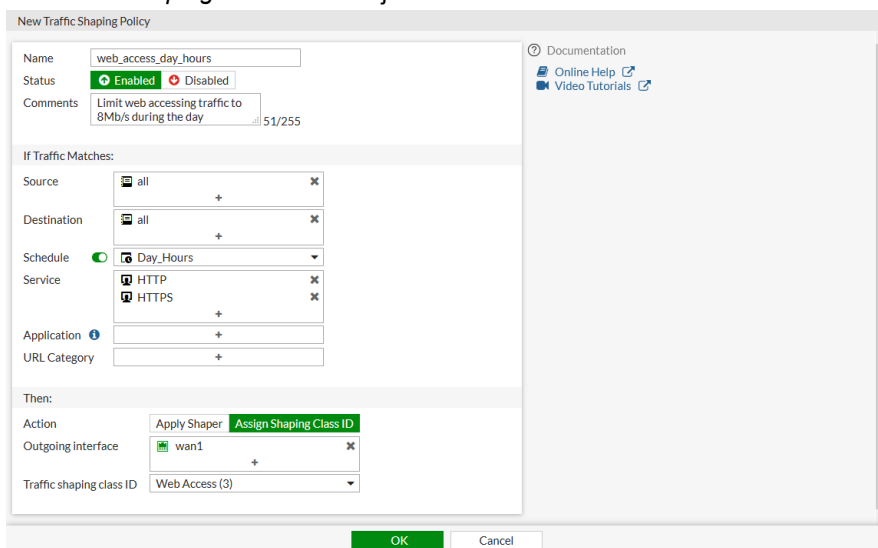
3. Configure a recurring schedule called *Day\_Hours* for everyday from 8:00 AM to 6:00 PM.
4. Click **OK**.

**To create a traffic shaping policy and class ID for the web accessing traffic in the GUI:**

1. Go to *Policy & Objects > Traffic Shaping Policy* and click *Create New*.
2. Enter a name for the policy, such as *web\_access\_day\_hours*.
3. Enable *Schedule* and select the schedule you just created.
4. Set *Service* to web accessing services, such as *HTTP* and *HTTPS*.
5. Set *Action* to *Assign Shaping Class ID*, and *Outgoing interface* to *wan1*
6. Click the *Traffic shaping class ID* drop down then click *Create*.
7. Enter a value for the *ID* (integer) and a description for the *Name*, such as *Web Access*.



8. Click **OK**.
9. Set *Traffic shaping class ID* to the just created class ID.

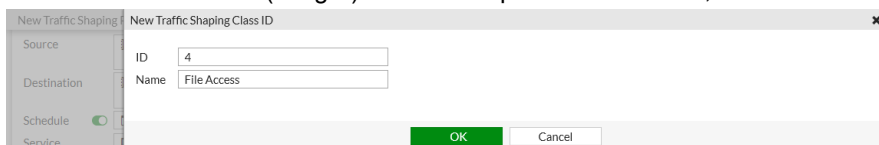


10. Configure the remaining settings as required.
11. Click **OK**.

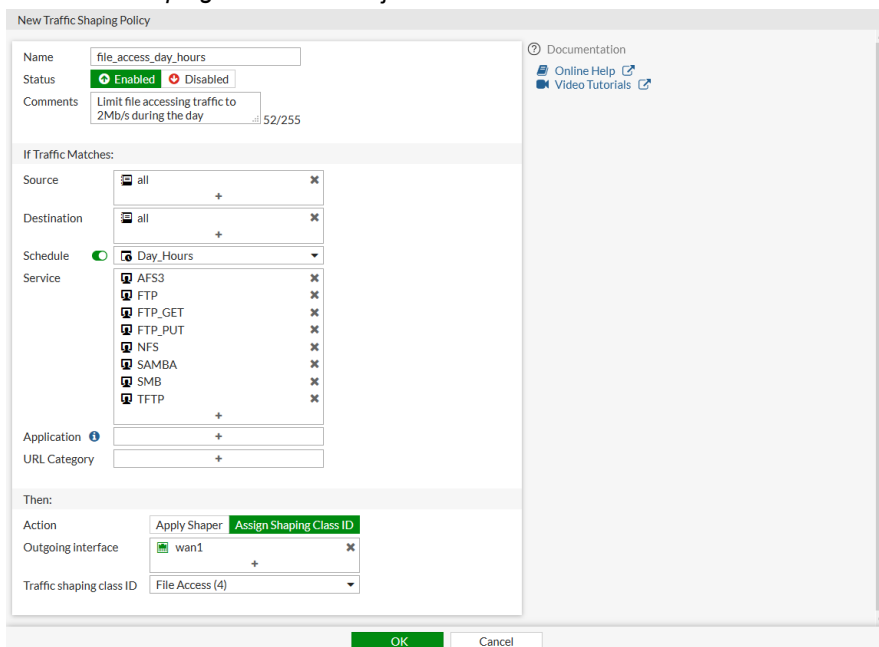
**To create a traffic shaping policy and class ID for the file accessing traffic in the GUI:**

1. Go to *Policy & Objects > Traffic Shaping Policy* and click *Create New*.
2. Enter a name for the policy, such as *file\_access\_day\_hours*.
3. Enable *Schedule* and select the schedule you just created.
4. Set *Service* to file accessing services, such as *ASF3*, *FTP* and *SMB*.
5. Set *Action* to *Assign Shaping Class ID*, and *Outgoing interface* to *wan1*
6. Click the *Traffic shaping class ID* drop down then click *Create*.

- Enter a value for the *ID* (integer) and a description for the *Name*, such as *File Access*.



- Click **OK**.
- Set *Traffic shaping class ID* to the just created class ID.



- Configure the remaining settings as required.
- Click **OK**.

### To put the traffic into shaping classes in the CLI:

- Create a recurring schedule:

```
config firewall schedule recurring
 edit "Day_Hours"
 set start 08:00
 set end 18:00
 set day sunday monday tuesday wednesday thursday friday saturday
 next
end
```

- Create the traffic class IDs:

```
config firewall traffic-class
 edit 3
 set class-name "Web Access"
 next
 edit 4
 set class-name "File Access"
 next
end
```

### 3. Create the web and file accessing traffic shaping policies:

```
config firewall shaping-policy
edit 2
 set name "web_access_day_hours"
 set comment "Limit web accessing traffic to 8Mb/s in day time"
 set service "HTTP" "HTTPS"
 set schedule "Day_Hours"
 set dstintf "wan1"
 set class-id 3
 set srcaddr "all"
 set dstaddr "all"
next
edit 3
 set name "file_access_day_hours"
 set comment "Limit file accessing traffic to 2Mb/s during the day"
 set service "AFS3" "FTP" "FTP_GET" "FTP_PUT" "NFS" "SAMBA" "SMB" "TFTP"
 set schedule "Day_Hours"
 set dstintf "wan1"
 set class-id 4
 set srcaddr "all"
 set dstaddr "all"
next
end
```

## Allocating bandwidth to the shaping classes

A traffic shaping profile defines the guaranteed and maximum bandwidths each class receives. In this example, file access can use up to 2 Mb/s and web access can use 8 Mb/s from 8:00 AM to 6:00 PM.

### To create a traffic shaping profile using the GUI:

1. Go to *Policy & Objects > Traffic Shaping Profile* and click *Create New*.

2. Enter a name for the profile, such as *Day\_Hours\_Profile*.

3. Configure a default traffic shaping class:

This class has a high priority, meaning that when the other classes have reached their guaranteed bandwidths, this default class will use the rest of the available bandwidth.

a. In the *Traffic Shaping Classes* table click *Create New*.

b. Click the *Traffic shaping class ID* drop down then click *Create*.

c. Enter a name for the class, such as *Default Access*.

d. Click *OK*.

e. Set *Traffic shaping class ID* to the just created class ID.



- f. Configure the following settings, then click **OK**:

<b>Guaranteed bandwidth</b>	30
<b>Maximum bandwidth</b>	100
<b>Priority</b>	High

4. Configure a web accessing traffic shaping class:

When other types of traffic are competing for bandwidth, this class is guaranteed to 6 Mb/s, or 60% of the bandwidth.

- In the *Traffic Shaping Classes* table click *Create New*.
- Configure the following settings, then click **OK**:

<b>Traffic shaping class ID</b>	Web Access
<b>Guaranteed bandwidth</b>	60
<b>Maximum bandwidth</b>	80
<b>Priority</b>	High

5. Configure a file accessing traffic shaping class:

When other types of traffic are competing for bandwidth, this group is guaranteed to 1 Mb/s, or 10% of the bandwidth.

- In the *Traffic Shaping Classes* table click *Create New*.
- Configure the following settings, then click **OK**:

<b>Traffic shaping class ID</b>	File Access
<b>Guaranteed bandwidth</b>	10
<b>Maximum bandwidth</b>	20
<b>Priority</b>	High

**Create Traffic Shaping Profile**

Name:  Comments:

**Traffic Shaping Classes**

Default	Class ID	Guaranteed Bandwidth	Maximum Bandwidth	Priority
Yes	Default Access (2)	30%	100%	High
	Web Access (3)	60%	80%	Medium
	File Access (4)	10%	20%	Medium

**Guaranteed Bandwidth Usage**

Legend: Default Access (2) (blue), Web Access (3) (yellow), File Access (4) (red), Not Allocated (grey)

6. Click OK.

### To create a traffic shaping profile using the CLI:

```
config firewall shaping-profile
 edit "Day_Hours_Profile"
 set default-class-id 2
 config shaping-entries
 edit 1
 set class-id 2
 set guaranteed-bandwidth-percentage 30
 set maximum-bandwidth-percentage 100
 next
 edit 2
 set class-id 3
 set priority medium
 set guaranteed-bandwidth-percentage 60
 set maximum-bandwidth-percentage 80
 next
 edit 3
 set class-id 4
 set priority medium
 set guaranteed-bandwidth-percentage 10
 set maximum-bandwidth-percentage 20
 next
 end
```

```

next
end

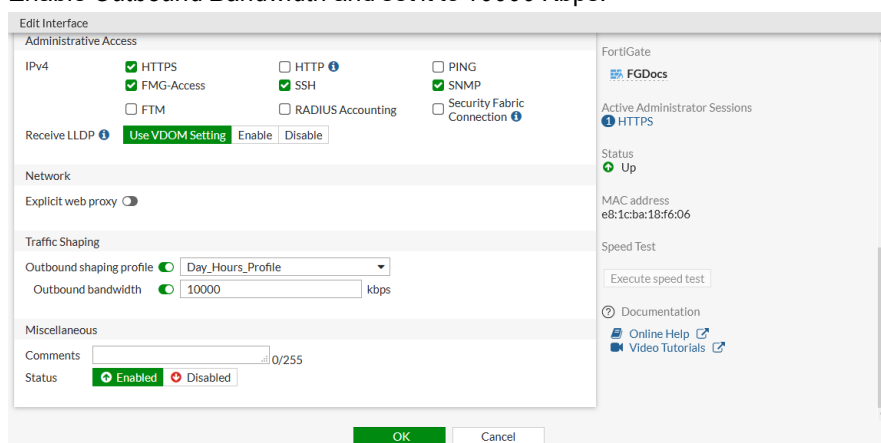
```

## Defining the available bandwidth on an interface

In this example, the link speed of the wan1 interface is 10 Mb/s.

### To set the bandwidth of the wan1 interface in the GUI:

1. Go to *Network > Interfaces*.
2. Edit the wan1 interface.
3. Under Traffic Shaping, enable *Outbound shaping profile* and select the profile that you just created, *Day\_Hours\_Profile*.
4. Enable *Outbound Bandwidth* and set it to *10000 Kbps*.



5. Click **OK**.

### To set the bandwidth of the wan1 interface in the CLI:

```

config system interface
 edit "wan1"

 set egress-shaping-profile "Day_Hours_Profile"
 set outbandwidth 10000

 next
end

```

## Diagnose commands

### To check that the specific traffic is put into the correct shaping group or class ID:

```
diagnose firewall iprope list 100015
```

### To check the speed limit for each class ID on an interface:

```
diagnose netlink interface list wan1
```

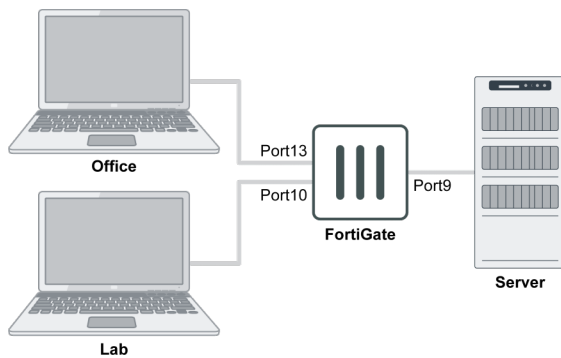
## Classifying traffic by source interface

In firewall shaping policies, you can classify traffic by source interface with the following command:

```
config firewall shaping-policy
edit 1
 set srcintf <interface_name>

next
end
```

### Sample configuration



For this example, there are two shaping policies:

- Policy 1 is for traffic from the Office to the Server, with the speed limited to 5 MB/s.
- Policy 2 is for traffic from the Lab to the Server, with the speed limited to 1 MB/s.

### To configure the traffic shaping policy:

```
config firewall shaping-policy
edit 1
 set name "Office_Speed_5MB"
 set service "ALL"
 set srcintf "port13"
 set dstintf "port9"
 set traffic-shaper "5MB/s"
 set traffic-shaper-reverse "5MB/s"
 set srcaddr "all"
 set dstaddr "all"
next
edit 2
 set name "Lab_Speed_1MB"
 set service "ALL"
 set srcintf "port10"
 set dstintf "port9"
 set traffic-shaper "1MB/s"
 set traffic-shaper-reverse "1MB/s"
 set srcaddr "all"
 set dstaddr "all"
next
end
```

## Configuring traffic class IDs

As of FortiOS 6.2.2, you can configure traffic class IDs with a descriptive name in the GUI or CLI. Class IDs can help you correlate traffic shaping policy and profile entries.

### GUI configurations

Within the GUI, there are three locations to configure the traffic class ID:

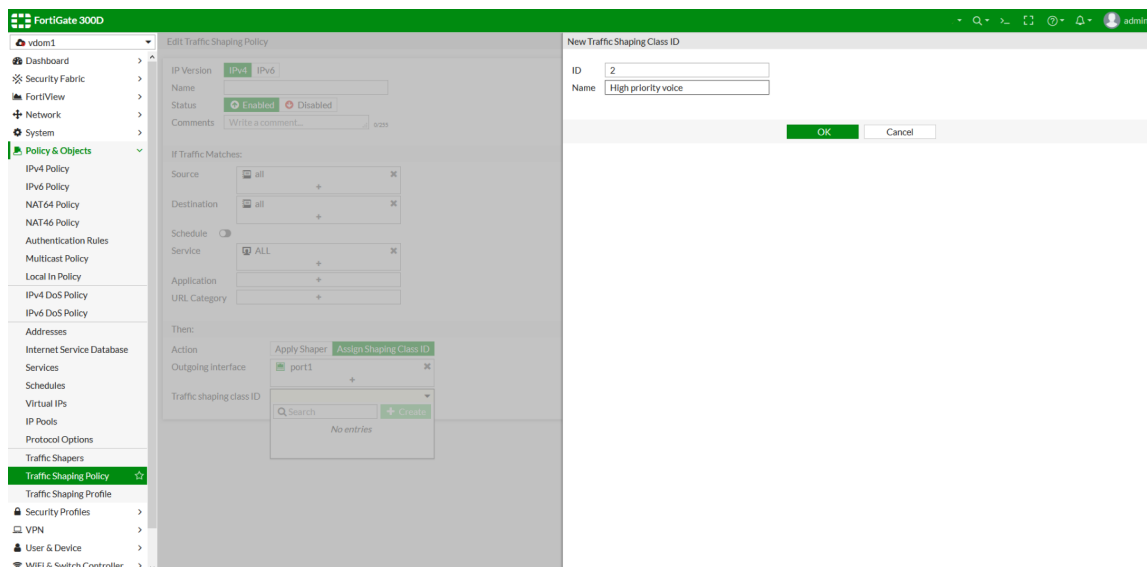
- [Traffic shaping policy](#)
- [Traffic shaping profile](#)
- [Interface](#)



*Assign Shaping Class ID* replaces the *Assign Group* functionality in earlier versions of FortiOS.

#### To configure the traffic class ID in a traffic shaping policy:

1. Go to *Policy & Objects > Traffic Shaping Policy*.
2. Edit an existing policy, or create a new one.
3. In the *Then: Action* section, click *Assign Shaping Class ID*.
4. In *Traffic shaping class ID*, click *Create*.
5. Enter a value for the *ID* (integer) and a description for the *Name*.
6. Click *OK* to save the class ID.

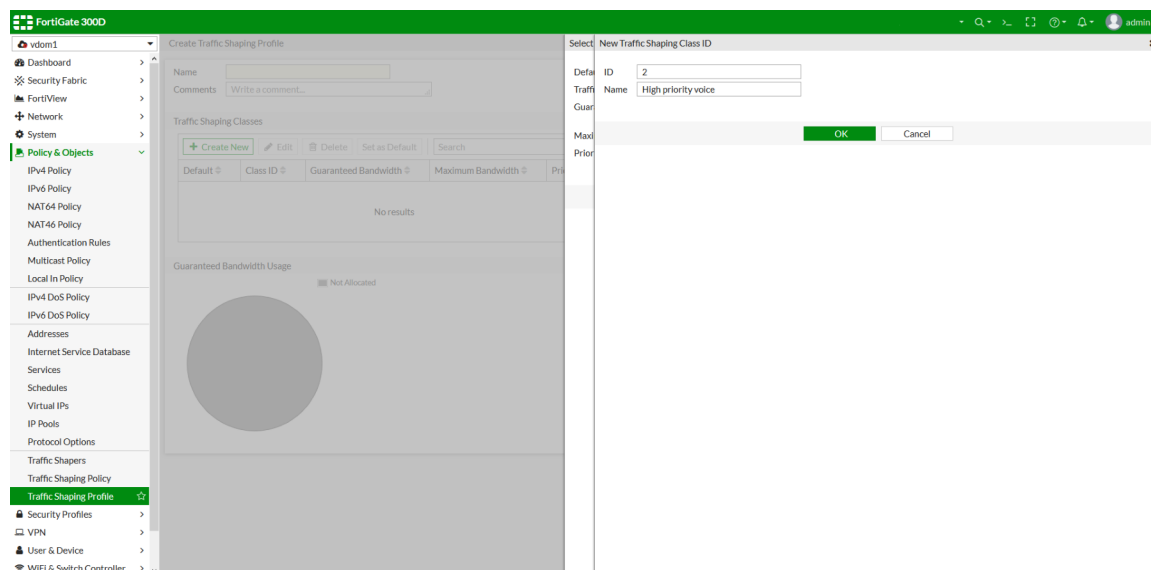


7. Configure the rest of the policy as needed.
8. Click *OK* to save the policy.

#### To configure the traffic class ID in a traffic shaping profile:

1. Go to *Policy & Objects > Traffic Shaping Profile*.
2. Edit an existing profile, or create a new one.

3. In the *Traffic Shaping Classes* section, click *Create New*. The *Select Traffic Shaping Class ID* window opens.
4. Click *Create*. The *New Traffic Shaping Class ID* window opens.
5. Enter a value for the *ID* (integer) and a description for the *Name*.
6. Click *OK* to save the class ID.

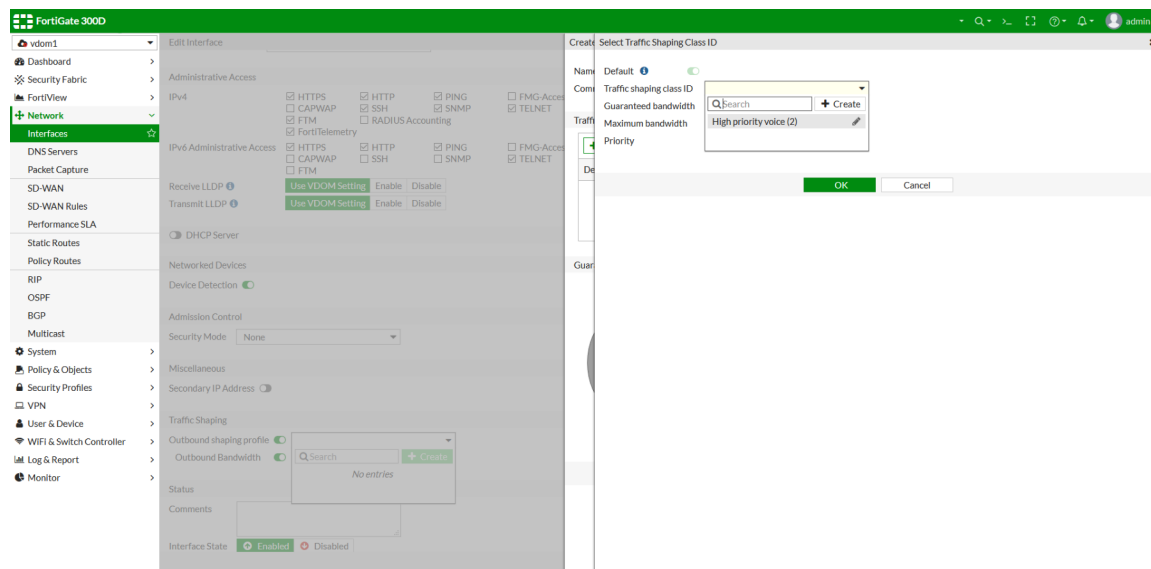


7. Click *OK* to add the class ID.
8. Configure the rest of the profile as needed.
9. Click *OK* to save the profile.

#### To configure the traffic class ID in an interface:

1. Go to *Network > Interfaces*.
2. Edit an existing interface, or create a new one.
3. In the *Traffic Shaping* section, enable *Outbound shaping profile* and *Outbound Bandwidth*.
4. Click *Create*. The *Create Traffic Shaping Profile* window opens.
5. Click *Create New*. The *Select Traffic Shaping Class ID* window opens.
6. Select an existing class ID, or create a new one.

7. Click **OK** to save the class ID.



8. Click **OK** to add the class ID .
9. Configure the rest of the interface as needed.
10. Click **OK** to save the interface.

## CLI configuration

To configure the traffic class ID in the CLI:

```
config firewall traffic-class
 edit 2
 set class-name "High priority voice."
 next
 ...
end
```

## Traffic shaping schedules

In a shaping policy, there are many matching criteria available for administrators to match a specific traffic and apply a traffic shaper or shaping group to the traffic, including using schedules. This feature gives shaping policy the ability to apply different shaping profiles at different times. Administrators can select a one-time schedule, recurring schedule, or schedule group.

*Schedule* is not a mandatory setting. If it is not set, then the current date and time are not used to match the traffic.

To configure a traffic shaping policy in the GUI:

1. Navigate to **Policy & Objects > Traffic Shaping Policy**.
2. Create or edit a **Traffic Shaping Policy**.

3. Enable *Schedule* and select a schedule option.

4. Configure other options and click *OK*.**To configure a traffic shaping policy in the CLI:**

```
config firewall schedule recurring
 edit "work-hours"
 set start 07:00
 set end 20:00
 set day monday tuesday wednesday thursday friday
 next
end

config firewall shaping-policy
 edit 1
 set name "demo"
 set service "ALL"
 set schedule "work-hours" <<< Can select schedule from one-time schedule, recurring
 schedule or schedule group
 set dstintf "port1"
 set traffic-shaper "high-priority"
 set traffic-shaper-reverse "high-priority"
 set srcaddr "all"
 set dstaddr "all"
 next
end
```

**To troubleshoot a traffic shaping policy in the CLI:**

The selected schedule is listed in the `iprope`.



```
diagnose firewall iprope list 100015

policy index=1 uuid_idx=0 action=accept
flag (0):
schedule (work-hours)
shapers: orig=high-priority(2/0/134217728) reply=high-priority(2/0/134217728)
cos_fwd=0 cos_rev=0
group=00100015 av=00000000 au=00000000 split=00000000
host=1 chk_client_info=0x0 app_list=0 ips_view=0
misc=0 dd_type=0 dd_mode=0
zone(1): 0 -> zone(1): 9
source(1): 0.0.0.0-255.255.255.255, uuid_idx=28,
dest(1): 0.0.0.0-255.255.255.255, uuid_idx=28,
service(1):
 [0:0x0:0/(0,65535)->(0,65535)] helper:auto
```

## QoS assignment and rate limiting for quarantined VLANs

When devices are quarantined, they are isolated from the rest of the network. However, they can still impact the network if not controlled beyond isolation. A quarantined host, which offers heavy traffic, could congest the network and create a DOS-style reduction in service to authorized hosts.

Within the quarantined VLAN, two restrictions are available within the network:

- Traffic policing (also known as rate limiting)
- QoS (Quality of Service) assignment (also known as priority assignment)

Each quarantined host's traffic can be subject to rate limiting and priority adjustment. This reduces the impact that any quarantined host can have on authorized traffic on the network.

### To configure QoS assignment and rate limiting for quarantined VLANs:

1. Configure a traffic policy, or use the default "quarantine" policy:

```
config switch-controller traffic-policy
 edit "quarantine"
 set description "Rate control for quarantined traffic"
 set guaranteed-bandwidth 163840
 set guaranteed-burst 8192
 set maximum-burst 163840
 set cos-queue 0
 next
end
```

2. Configure an interface:

```
config system interface
 edit "qtn.aggr1"
 set vdom "root"
 set ip 10.254.254.254 255.255.255.0
 set description "Quarantine VLAN"
 set security-mode captive-portal
 set replacemsg-override-group "auth-intf-qtn.aggr1"
 set device-identification enable
 set snmp-index 30
 set switch-controller-access-vlan enable
```

```
 set switch-controller-traffic-policy "quarantine"
 set color 6
 set interface "aggr1"
 set vlanid 4093
 next
end
```

By default, `switch-controller-traffic-policy` is empty. You need to apply the necessary traffic policy (not only limited to "quarantine").

## Weighted random early detection queuing

You can use the weighted random early detection (WRED) queuing function within traffic shaping.

This topic includes three parts:

- [Traffic shaping with queuing](#)
- [Burst control in queuing mode](#)
- [Multi-stage DSCP marking and class ID in traffic shapers](#)

You cannot configure or view WRED in the GUI; you must use the CLI.



WRED is not supported when traffic is offloaded to an NPU.

---

### Traffic shaping with queuing

Traffic shaping has a queuing option. Use this option to fine-tune the queue by setting the profile queue size or performing random early drop (RED) according to queue usage.

This example shows setting the profile queue size limit to 5 so that the queue can contain a maximum of five packets and more packets are dropped.

#### To set the profile queue size limit:

```
config firewall shaping-profile
edit "profile"
 set type queuing
 set default-class-id 31
 config shaping-entries
 edit 31
 set class-id 31
 set guaranteed-bandwidth-percentage 5
 set maximum-bandwidth-percentage 10
 set limit 5 <range from 5 to 10000; default: 1000>
 next
 end
next
end
```

This example shows performing RED according to queue usage by setting `red-probability`, `min`, and `max`. Setting `red-probability` to 10 means start to drop packets when queue usage reaches the `min` setting. When queue usage reaches the `max` setting, drop 10% of the packets.

- Level 1: when queue is less than `min` packets, drop 0% of packets.
- Level 2: when queue reaches `min` packets, start to drop packets.
- Level 3: when queue usage is between `min` and `max` packets, drop 0–10% of packets by proportion.
- Level 4: when queue (average queue size) is more than `max` packets, drop 100% of packets.

**To set RED according to queue usage:**

```
config firewall shaping-profile
 edit "profile"
 set type queuing
 set default-class-id 31
 config shaping-entries
 edit 31
 set class-id 31
 set guaranteed-bandwidth-percentage 5
 set maximum-bandwidth-percentage 10
 set red-probability 10 <range from 0 to 20; default: 0 no drop>
 set min 100 <range from 3 to 3000>
 set max 300 <range from 3 to 3000>
 next
 end
 next
end
```

**To troubleshoot this function, use the following diagnose commands:**

```
diagnose netlink intf-class list <intf>
diagnose netlink intf-qdisc list <intf>
```

**Burst control in queuing mode**

In a hierarchical token bucket (HTB) algorithm, each traffic class has buckets to allow a burst of traffic. The maximum burst is determined by the bucket size `burst` (for guaranteed bandwidth) and `cburst` (for maximum bandwidth). The shaping profile has `burst-in-msec` and `cburst-in-msec` parameters for each shaping entry (`class id`) to control the bucket size.

This example uses the outbandwidth of the interface as 1 Mbps and the maximum bandwidth of class is 50%.

$\text{burst} = \text{burst-in-msec} \times \text{guaranteed bandwidth} = 100 \text{ ms} \times 1 \text{ Mbps} \times 50\% = 50000 \text{ b} = 6250 \text{ B}$

$\text{cburst} = \text{cburst-in-msec} \times \text{maximum bandwidth} = 200 \text{ ms} \times 1 \text{ Mbps} \times 50\% = 100000 \text{ b} = 12500 \text{ B}$

The following example sets `burst-in-msec` to 100 and `cburst-in-msec` to 200.

**To set burst control in queuing mode:**

```
config firewall shaping-profile
 edit "profile"
 set type queuing
 set default-class-id 31
 config shaping-entries
 edit 31
 set class-id 31
 set guaranteed-bandwidth-percentage 5
 set maximum-bandwidth-percentage 50
```

```

 set burst-in-msec 100 <range from 0 to 2000>
 set cburst-in-msec 200 <range from 0 to 2000>
 next
end
next
end

```

## Multi-stage DSCP marking and class ID in traffic shapers

Traffic shapers have a multi-stage method so that packets are marked with a different differentiated services code point (DSCP) and `class id` at different traffic speeds. Marking packets with a different DSCP code is for the next hop to classify the packets. The FortiGate benefits by marking packets with a different `class id`. Combined with the egress interface shaping profile, the FortiGate can handle the traffic differently according to its `class id`.

Rule	DSCP code	Class ID
speed < guarantee bandwidth	diffservcode	class id in shaping policy
guarantee bandwidth < speed < exceed bandwidth	exceed-dscp	exceed-class-id
exceed bandwidth < speed	maximum-dscp	exceed-class-id

This example sets the following parameters:

- When the current bandwidth is less than 50 Kbps, mark packets with `diffservcode 100000` and set `class id` to 10.
- When the current bandwidth is between 50 Kbps and 100 Kbps, mark packets with `exceed-dscp 111000` and set `exceed-class-id` to 20.
- When the current bandwidth is more than 100 Kbps, mark packets with `maximum-dscp 111111` and set `exceed-class-id` to 20.

### To set multi-stage DSCP marking and class ID in a traffic shaper:

```

config firewall shaper traffic-shaper
 edit "50k-100k-150k"
 set guaranteed-bandwidth 50
 set maximum-bandwidth 150
 set diffserv enable
 set dscp-marking-method multi-stage
 set exceed-bandwidth 100
 set exceed-dscp 111000
 set exceed-class-id 20
 set maximum-dscp 111111
 set diffservcode 100000
 next
end

config firewall shaping-policy
 edit 1
 set service "ALL"
 set dstintf PORT2
 set srcaddr "all"
 set dstaddr "all"
 set class-id 10
 next
end

```

Traffic shapers also have an `overhead` option that defines the per-packet size overhead used in rate computation.

**To set the traffic shaper overhead option:**

```
config firewall shaper traffic-shaper
 edit "testing"
 set guaranteed-bandwidth 50
 set maximum-bandwidth 150
 set overhead 14 <range from 0 to 100>
 next
end
```

## Examples

**Enabling RED for FTP traffic from QA**

This first example shows how to enable RED for FTP traffic from QA. This example sets a maximum of 10% of the packets to be dropped when queue usage reaches the maximum value.

**To configure the firewall address:**

```
config firewall address
 edit QA_team
 set subnet 10.1.100.0/24
 next
end
```

**To set the shaping policy to classify traffic into different class IDs:**

```
config firewall shaping-policy
 edit 1
 set service HTTPS HTTP
 set dstintf port1
 set srcaddr QA_team
 set dstaddr all
 set class-id 10
 next
 edit 2
 set service FTP
 set dstintf port1
 set srcaddr QA_team
 set dstaddr all
 set class-id 20
 next
end
```

**To set the shaping policy to define the speed of each class ID:**

```
config firewall shaping-profile
 edit QA_team_profile
 set type queuing
 set default-class-id 30
 config shaping-entries
 edit 1
```

```
 set class-id 10
 set guaranteed-bandwidth-percentage 50
 set maximum-bandwidth-percentage 100
 next
 edit 2
 set class-id 20
 set guaranteed-bandwidth-percentage 30
 set maximum-bandwidth-percentage 60
 set red-probability 10
 next
 edit 3
 set class-id 30
 set guaranteed-bandwidth-percentage 20
 set maximum-bandwidth-percentage 50
 next
end
next
end
```

### To apply the shaping policy to the interface:

```
config sys interface
 edit port1
 set outbandwidth 10000
 set egress-shaping-profile QA_team_profile
 next
end
```

### To use diagnose commands to troubleshoot:

```
diagnose netlink intf-class list port1
class htb 1:1 root rate 1250000Bps ceil 1250000Bps burst 1600B/8 mpu 0B overhead 0B cburst
1600B/8 mpu 0B overhead 0B level 7 buffer [00004e20] cbuffer [00004e20]
Sent 11709 bytes 69 pkt (dropped 0, overlimits 0 requeues 0)
rate 226Bps 2pps backlog 0B 0p
lended: 3 borrowed: 0 giants: 0
tokens: 18500 ctokens: 18500
class htb 1:10 parent 1:1 leaf 10: prio 1 quantum 62500 rate 625000Bps ceil 1250000Bps burst
1600B/8 mpu 0B overhead 0B cburst 1600B/8 mpu 0B overhead 0B level 0 buffer [00009c40]
cbuffer [00004e20]
Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
rate 0Bps 0pps backlog 0B 0p
lended: 0 borrowed: 0 giants: 0
tokens: 40000 ctokens: 20000
class htb 1:20 parent 1:1 leaf 20: prio 1 quantum 37500 rate 375000Bps ceil 750000Bps burst
1599B/8 mpu 0B overhead 0B cburst 1599B/8 mpu 0B overhead 0B level 0 buffer [0001046a]
cbuffer [00008235]
Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
rate 0Bps 0pps backlog 0B 0p
lended: 0 borrowed: 0 giants: 0
tokens: 66666 ctokens: 33333
class htb 1:30 parent 1:1 leaf 30: prio 1 quantum 25000 rate 250000Bps ceil 625000Bps burst
1600B/8 mpu 0B overhead 0B cburst 1600B/8 mpu 0B overhead 0B level 0 buffer [000186a0]
cbuffer [00009c40]
Sent 11709 bytes 69 pkt (dropped 0, overlimits 0 requeues 0)
rate 226Bps 2pps backlog 0B 0p
```

```
lended: 66 borrowed: 3 giants: 0
tokens: 92500 ctokens: 37000
class red 20:1 parent 20:0

diagnose netlink intf-qdisc list port1
qdisc htb 1: root refcnt 5 r2q 10 default 30 direct_packets_stat 0 ver 3.17
 Sent 18874 bytes 109 pkt (dropped 0, overlimits 5 requeues 0)
 backlog 0B 0p
qdisc pfifo 10: parent 1:10 refcnt 1 limit 1000p
 Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
 backlog 0B 0p
qdisc red 20: parent 1:20 refcnt 1 limit 4000000B min 300000B max 1000000B ewma 9 Plog 23
 Scell_log 20 flags 0
 Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
 backlog 0B 0p
 marked 0 early 0 pdrop 0 other 0
qdisc pfifo 30: parent 1:30 refcnt 1 limit 1000p
 Sent 18874 bytes 109 pkt (dropped 0, overlimits 0 requeues 0)
 backlog 0B 0p
```

### Marking QA traffic with a different DSCP

This second example shows how to mark QA traffic with a different DSCP according to real-time traffic speed.

#### To configure the firewall address:

```
config firewall address
 edit QA_team
 set subnet 10.1.100.0/24
 next
end
```

#### To configure the firewall shaper traffic shaper:

```
config firewall shaper traffic-shaper
 edit "500k-1000k-1500k"
 set guaranteed-bandwidth 500
 set maximum-bandwidth 1500
 set diffserv enable
 set dscp-marking-method multi-stage
 set exceed-bandwidth 1000
 set exceed-dscp 111000
 set maximum-dscp 111111
 set diffservcode 100000
 next
end

config firewall shaping-policy
 edit QA_team
 set service "ALL"
 set dstintf port1
 set traffic-shaper "500k-1000k-1500k"
 set traffic-shaper-reverse "500k-1000k-1500k"
 set srcaddr "QA_team"
 set dstaddr "all"
```

```
 next
end
```



# Security Profiles

This section contains information about configuring FortiGate security features, including:

- [Antivirus on page 907](#)
- [Web filter on page 947](#)
- [DNS filter on page 998](#)
- [Application control on page 1021](#)
- [Intrusion prevention on page 1028](#)
- [Email filter on page 1041](#)
- [Data leak prevention on page 1059](#)
- [VoIP solutions on page 1066](#)
- [ICAP on page 1077](#)
- [Web application firewall on page 1080](#)
- [Inspection modes on page 1084](#)
- [Overrides on page 1101](#)
- [Custom signatures on page 1111](#)



If you are unable to view a security profile feature, go to *System > Feature Visibility* to enable it.

---

## Antivirus

FortiOS offers the unique ability to implement both flow-based and proxy-based antivirus concurrently, depending on the traffic type, users, and locations. Flow-based antivirus offers higher throughput performance, while proxy-based solutions are useful to mitigate stealthy malicious codes.

FortiOS includes two preloaded antivirus profiles:

- *default*
- *wifi-default*

You can customize these profiles, or you can create your own to inspect certain protocols, remove viruses, analyze suspicious files with FortiSandbox, and apply botnet protection to network traffic. Once configured, you can add the antivirus profile to a firewall policy.



This functionality requires a subscription to FortiGuard Antivirus.

---

Starting from 6.2, for oversized files, the UTM scan strategy used in proxy mode for the HTTP, HTTPS, FTP, FTPS, and SSH protocols is best effort in both default and legacy scan modes. In the FortiGate memory allocation based on the

oversize limit and uncompressed oversize limit defined in the protocol options, the FortiGate scans buffered files as much as it can. This strategy improves the effectiveness of the malware detection, and provides better security by scanning whole or partial files that would be bypassed if oversized files were bypassed.

The following topics provide information about antivirus profiles:

- [Content disarm and reconstruction for antivirus on page 908](#)
- [FortiGuard outbreak prevention for antivirus on page 911](#)
- [External malware block list for antivirus on page 913](#)
- [Checking flow antivirus statistics on page 916](#)
- [CIFS support on page 918](#)
- [Databases on page 925](#)

The following topics provide information about sandbox inspection with antivirus:

- [Using FortiSandbox appliance with antivirus on page 926](#)
- [Using FortiSandbox Cloud with antivirus on page 936](#)

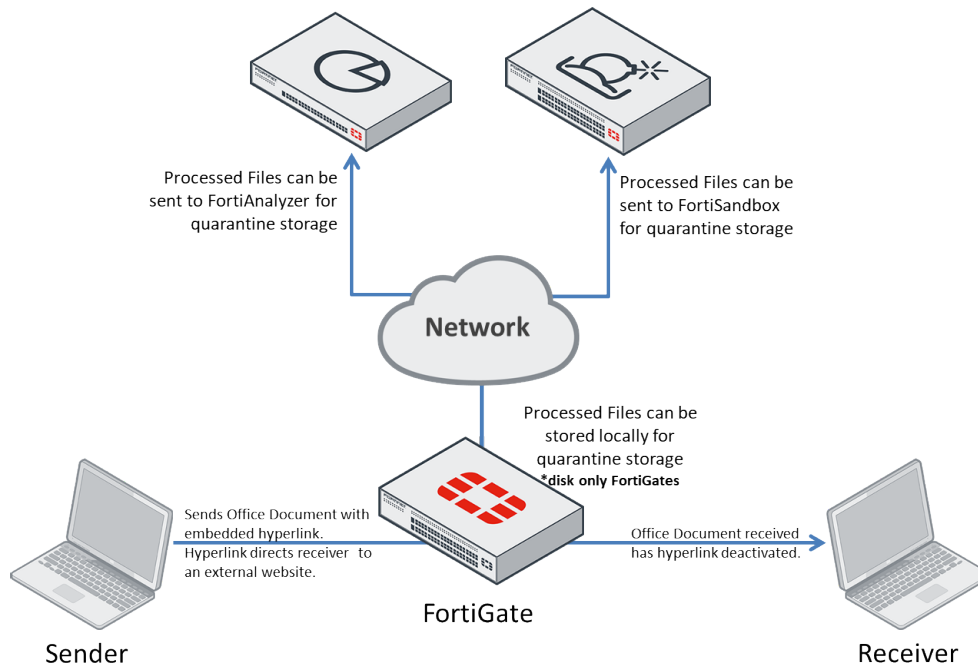
## Content disarm and reconstruction for antivirus

Content disarm and reconstruction (CDR) allows the FortiGate to sanitize Microsoft Office documents and PDF files by removing active content, such as hyperlinks, embedded media, javascript, macros, and so on (disarm) from the files without affecting the integrity of its textual content (reconstruction). It allows network admins to protect their users from malicious document files.

- CDR can be performed on Microsoft Office document and PDF files, including those that are in ZIP archives.
- CDR is supported on HTTP, SMTP, POP3, IMAP. SMTP splice and client-comfort mode are not supported.
- CDR does not support flow-based inspection modes.
- Local disk CDR quarantine can be used on FortiGate models that contain a hard disk or disks.

Files processed by CDR can have the original copy quarantined on the FortiGate, allowing administrators to observe them. The original copies can also be obtained in the event of a false positive.

## Network topology example

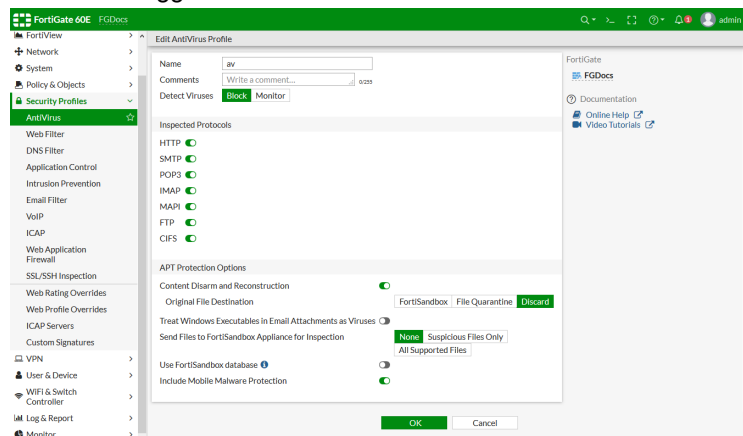


## Configuring the feature

In order to configure antivirus to work with CDR, you must enable CDR on your antivirus profile, set the quarantine location, and then fine-tune the CDR detection parameters.

**To enable CDR on your antivirus profile:**

1. Go to *Security Profiles > AntiVirus*.
2. Edit an antivirus profile, or create a new one.
3. Enable the toggle for *Content Disarm and Reconstruction* under *APT Protection Options*.



**To set a quarantine location:**

1. Go to *Security Profiles > AntiVirus*.
2. Edit an antivirus profile, or create a new one.
3. Select a quarantine location from the available options: *Discard*, *File Quarantine*, or *FortiSandbox*.

<b>Discard</b>	The default setting, which discards the original document file.
<b>File Quarantine</b>	Saves the original document file to disk (if possible) or a connected FortiAnalyzer based on the FortiGate's log settings, visible through <i>Config Global &gt; Config Log FortiAnalyzer Setting</i> .
<b>FortiSandbox</b>	Saves the original document file to a connected FortiSandbox.

4. Click *Apply*.

**To fine-tune CDR detection parameters in the CLI:**

- Select which active content to detect/process:  
By default, all active office and PDF content types are enabled. To fine-tune CDR to ignore certain content, you must disable that particular content parameter. The example below configures the CDR to ignore Microsoft Office macros.

```
config antivirus profile
 edit av
 config content-disarm
 set office-macro disable
 end
 next
end
```

- Detect but do not modify active content:  
By default, CDR will disarm any detected documents containing active content. To prevent CDR from disarming documents, you can set it to operate in detect-only mode. To do this, the option *detect-only* must be enabled.

```
config antivirus profile
 edit av
 config content-disarm
 set detect-only enable
 end
 next
end
```

- Disable the CDR cover page:  
By default, a cover page will be attached to the file's content when the file has been processed by CDR. To disable the cover page, the *cover-page* parameter needs to be disabled.

```
config antivirus profile
 edit av
 config content-disarm
 set cover-page disable
 end
 next
end
```

## FortiGuard outbreak prevention for antivirus

FortiGuard outbreak prevention allows the FortiGate antivirus database to be subsidized with third-party malware hash signatures curated by the FortiGuard. The hash signatures are obtained from external sources such as VirusTotal, Symantec, Kaspersky, and other third-party websites and services.

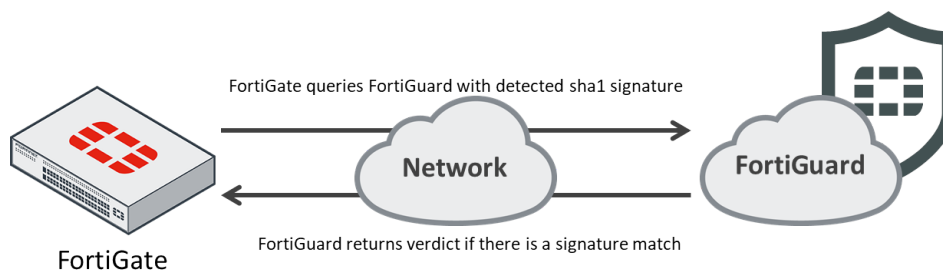
This feature provides the mechanism for antivirus to query the FortiGuard with the hash of a scanned file. If the FortiGuard returns a match from its many curated signature sources, the scanned file is deemed to be malicious.

The concept of FortiGuard outbreak prevention is to detect zero-day malware in a collaborative approach.

### Support and limitations

- FortiGuard outbreak prevention can be used in both proxy-based and flow-based policy inspections across all supported protocols.
- FortiGuard outbreak prevention does not support AV in quick scan mode.
- FortiGate must be registered with a valid FortiGuard outbreak prevention license before this feature can be used.

### Network topology example



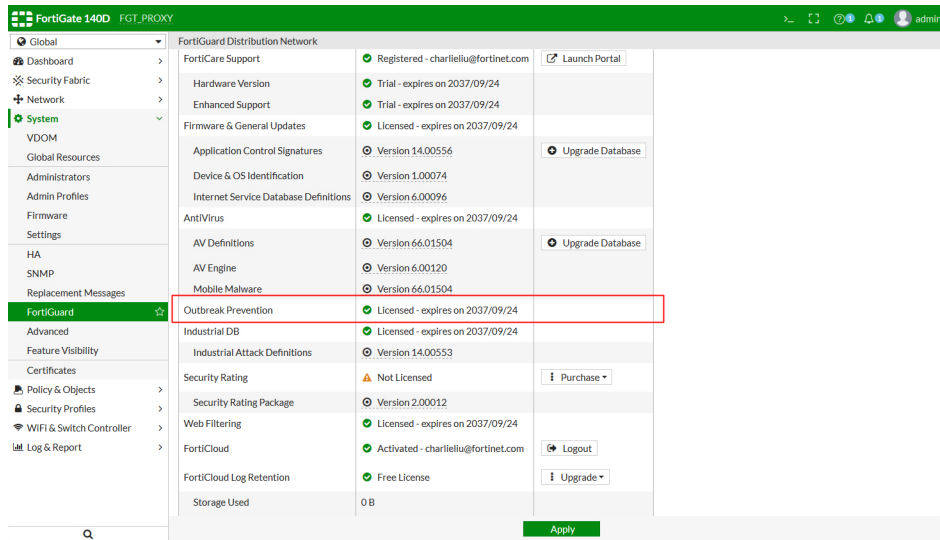
### Configuring the feature

In order for antivirus to work with an external block list, you must register the FortiGate with a FortiGuard outbreak prevention license and enable FortiGuard outbreak prevention in the antivirus profile.

#### To obtain/renew a FortiGuard antivirus license:

1. See the following link for instructions on how to purchase or renew a FortiGuard outbreak prevention license:  
<https://video.fortinet.com/products/fortigate/6.0/how-to-purchase-or-renew-fortiguard-services-6-0>

- Once the license has been activated, you can verify its status by going to *Global > System > FortiGuard*.



To enable FortiGuard outbreak prevention in the antivirus profile:

- Go to *Security Profiles > AntiVirus*.
- Edit an antivirus profile, or create a new one.
- Select the toggle to enable *Use FortiGuard Outbreak Prevention Database*.
- Click *Apply*.

## Diagnostics and debugging

- Check if FortiGate has outbreak prevention license:

```
diagnose debug rating
Locale : english
```

```
Service : Web-filter
Status : Enable
License : Contract
```

```
Service : Antispam
Status : Disable
```

```
Service : Virus Outbreak Prevention
Status : Enable
License : Contract
```

```
-- Server List (Tue Feb 19 16:36:15 2019) --
```

IP	Weight	RTT	Flags	TZ	Packets	Curr Lost	Total Lost	
Updated Time								
192.168.100.185	-218	2	DI	-8	113	0	0	Tue
Feb 19 16:35:55 2019								

- Scanunit daemon showing outbreak prevention verdict:

```
diagnose debug application scanunit -1
Debug messages will be on for 30 minutes.

diagnose debug enable

su 4739 job 1 open
su 4739 req vfid 1 id 1 ep 0 new request, size 313, policy id 1, policy type 0
su 4739 req vfid 1 id 1 ep 0 received; ack 1, data type: 0
su 4739 job 1 request info:
su 4739 job 1 client 10.1.100.11:39412 server 172.16.200.44:80
su 4739 job 1 object_name 'zhvo_test.com'
su 4739 file-typing NOT WANTED options 0x0 file_filter no
su 4739 enable databases 0b (core mmdb extended)
su 4739 job 1 begin http scan
su 4739 scan file 'zhvo_test.com' bytes 68
su 4739 job 1 outbreak-prevention scan, level 0, filename 'zhvo_test.com'
su 4739 scan result 0
su 4739 job 1 end http scan
su 4739 job 1 inc pending tasks (1)
su 4739 not wanted for analytics: analytics submission is disabled (m 0 r 0)
su 4739 job 1 suspend
su 4739 outbreak-prevention recv error
su 4739 ftgd avquery id 0 status 1
su 4739 job 1 outbreak-prevention infected entryid=0
su 4739 report AVQUERY infection priority 1
su 4739 insert infection AVQUERY SUCCEEDED loc (nil) off 0 sz 0 at index 0 total
infections 1 error 0
su 4739 job 1 dec pending tasks 0
su 4739 job 1 send result
su 4739 job 1 close
su 4739 outbreak-prevention recv error
```

## External malware block list for antivirus

The external malware block list is a new feature introduced in FortiOS 6.2.0, which falls under the umbrella of outbreak prevention.

This feature provides another means of supporting the AV Database by allowing users to add their own malware signatures in the form of MD5, SHA1, and SHA256 hashes.

This feature provides a mechanism for antivirus to retrieve an external malware hash list from a remote server and polls the hash list every *n* minutes for updates.

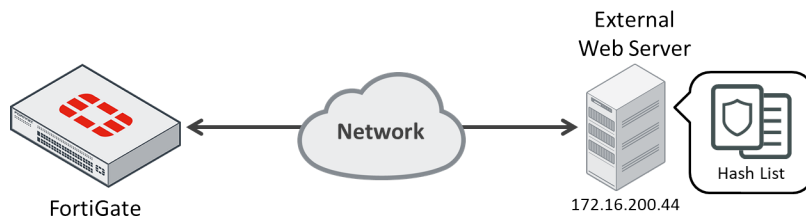
### Support and limitations

Malware detection using the external malware block list can be used in both proxy-based and flow-based policy inspections.

Just like FortiGuard outbreak prevention, external dynamic block list is not supported in AV default scan mode.

Using different types of hashes simultaneously may slow down the performance of malware scanning. For this reason, users are recommended to only using one type of hash (either MD5, SHA1, or SHA256), not all three simultaneously.

## Network topology example



## Configuring the feature

### To configure antivirus to work with external block list:

#### 1. Create the malware hash list

The malware hash list follows a strict format in order for its contents to be valid. Malware hash signature entries must be separated into each line. A valid signature needs to follow the format below:

```
MD5 Entry with hash description
aa67243f746e5d76f68ec809355ec234 md5_sample1

SHA1 Entry with hash description
a57983cb39e25ab80d7d3dc05695dd0ee0e49766 sha1_sample2

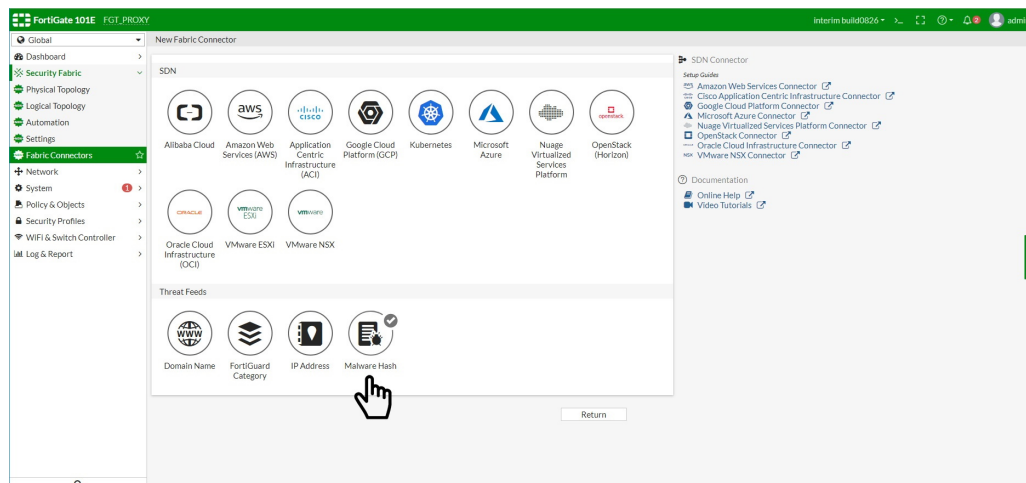
SHA256 Entry with hash description
ae9bc0b4c5639d977d720e4271da06b50f7c60d1e2070e9c75cc59ab30e49379 sha256_sample1

Entry without hash description
0289b0d967cb7b1fb1451339c7b9818a621903090e0020366ab415c549212521

Invalid entries
7688499dc71b932feb126347289c0b8a_md5_sample2
7614e98badca10b5e2d08f8664c519b7a906fbd5180ea5d04a82fce9796a4b87sha256_sample3
```

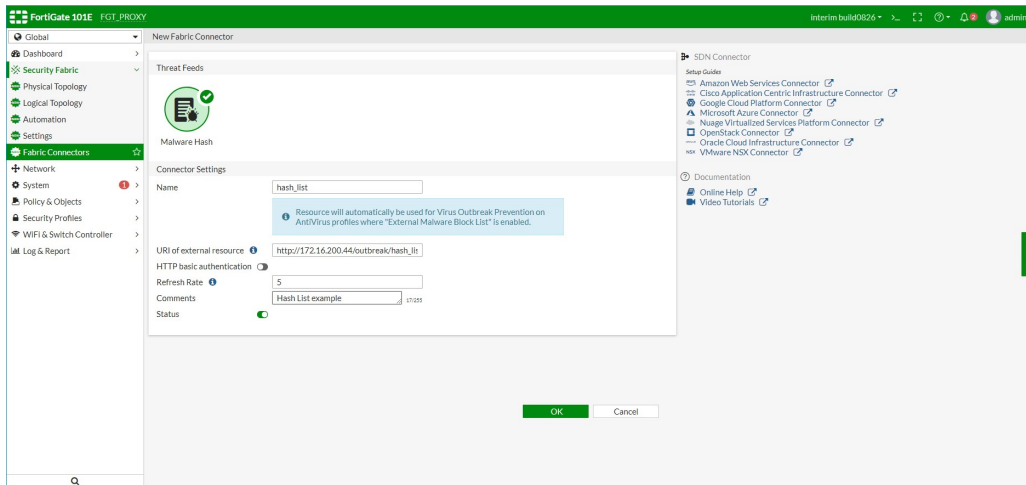
#### 2. Configure the external malware block list source:

- a. Go to *Global > Security Fabric > Fabric Connectors* and click *Create New*.
- b. Select *Malware Hash*.





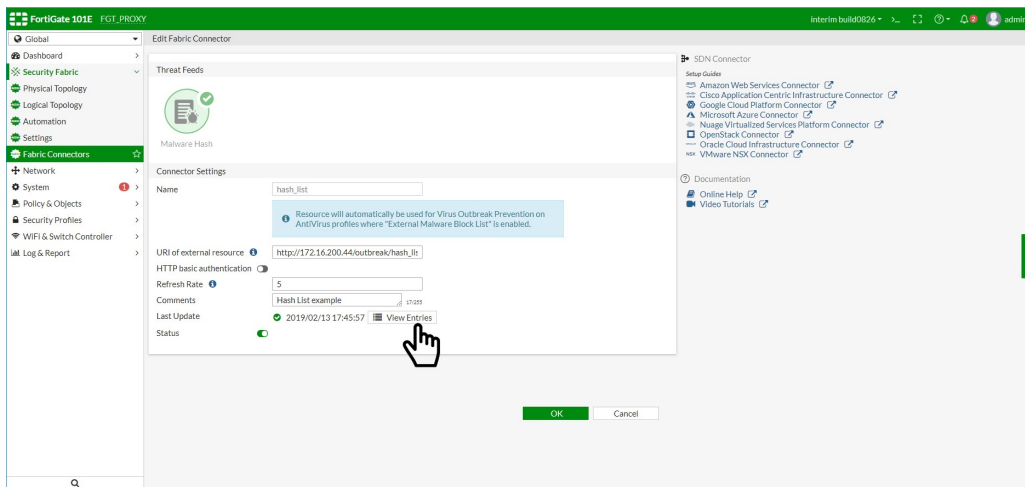
- c. Fill out the fields as shown. The URI must point to the malware hash list on the remote server.



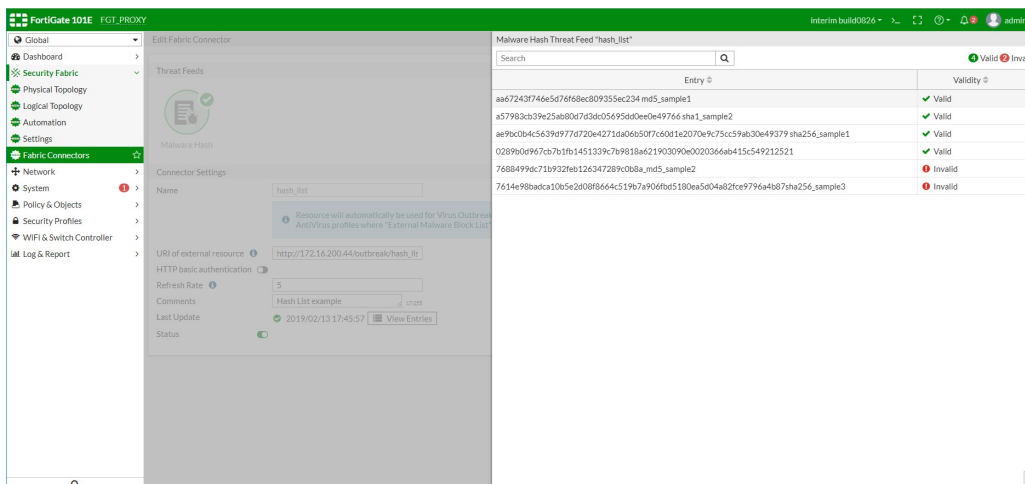
- d. Click OK.

The malware hash source object is now created.

To view entries inside the malware block list, click the *View Entries* button:



The malware hash threat feed is shown (*hash\_list*):



### 3. Enable the external malware block list in the antivirus profile:

```
config antivirus profile
 edit <av_profile>
 config outbreak-prevention
 set external-blocklist enable
 end
 next
end
```

Antivirus is now ready to use the external malware block list.

## Diagnostics and debugging

Check if the `scanunit` daemon has updated itself with the external hashes:

```
FGT_PROXY # config global
FGT_PROXY (global) # diagnose sys scanunit malware-list list
md5 'aa67243f746e5d76f68ec809355ec234' profile 'hash_list' description 'md5_sample1'
sha1 'a57983cb39e25ab80d7d3dc05695dd0ee0e49766' profile 'hash_list' description 'sha1_sample2'
sha256 '0289b0d967cb7b1fb1451339c7b9818a621903090e0020366ab415c549212521' profile 'hash_list' description ''
sha256 'ae9bc0b4c5639d977d720e4271da06b50f7c60d1e2070e9c75cc59ab30e49379' profile 'hash_list' description 'sha256_sample1'
```

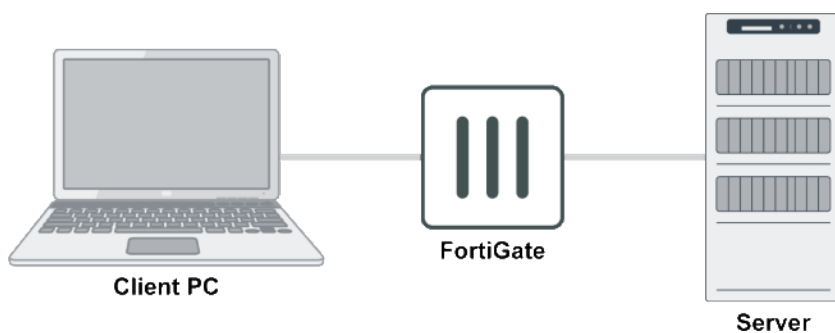
## Checking flow antivirus statistics

This feature provides a flow antivirus statistics check, and an API for SNMP to get AV statistics.

Two CLI commands are used to show and clear the antivirus statistics:

```
diagnose ips av stats show
diagnose ips av stats clear
```

This example uses the following topology:



### To check flow antivirus statistics:

#### 1. Create an antivirus profile:

```
config antivirus profile
 edit "av-test"
 config http
 set options scan avmonitor
```

```
 end
 config ftp
 set options scan quarantine
 end
 next
end
```

**2. Enable the profile on a firewall policy:**

```
config firewall policy
 edit 1
 set name "policy1"
 set srcintf "port2"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set utm-status enable
 set fsso disable
 set av-profile "av-test"
 set ssl-ssh-profile "custom-deep-inspection"
 set nat enable
 next
end
```

**3. On the client PC, download the EICAR Standard Anti-Virus Test File via HTTP.**

**4. Check the antivirus statistics on the FortiGate. As the action is set to monitor for HTTP, HTTP virus detected is increased by 1:**

```
diagnose ips av stats show
AV stats:
HTTP virus detected: 1
HTTP virus blocked: 0
SMTP virus detected: 0
SMTP virus blocked: 0
POP3 virus detected: 0
POP3 virus blocked: 0
IMAP virus detected: 0
IMAP virus blocked: 0
NNTP virus detected: 0
NNTP virus blocked: 0
FTP virus detected: 0
FTP virus blocked: 0
SMB virus detected: 0
SMB virus blocked: 0
```

**5. On the client PC, download the EICAR file via FTP.**

**6. Check the antivirus statistics on the FortiGate. As the action is set to quarantine for FTP, FTP virus detected and FTP virus blocked are both increased by 1:**

```
diagnose ips av stats show
AV stats:
HTTP virus detected: 1
HTTP virus blocked: 0
SMTP virus detected: 0
```

```
SMTP virus blocked: 0
POP3 virus detected: 0
POP3 virus blocked: 0
IMAP virus detected: 0
IMAP virus blocked: 0
NNTP virus detected: 0
NNTP virus blocked: 0
FTP virus detected: 1
FTP virus blocked: 1
SMB virus detected: 0
SMB virus blocked: 0
```

## 7. Check the antivirus statistics using snmpwalk:

```
root:~# snmpwalk -c public -v 1 10.1.100.6 1.3.6.1.4.1.12356.101.8.2.1.1
iso.3.6.1.4.1.12356.101.8.2.1.1.1.1 = Counter32: 2 (fgAvVirusDetected)
iso.3.6.1.4.1.12356.101.8.2.1.1.2.1 = Counter32: 1 (fgAvVirusBlocked)
iso.3.6.1.4.1.12356.101.8.2.1.1.3.1 = Counter32: 1 (fgAvHTTPVirusDetected)
iso.3.6.1.4.1.12356.101.8.2.1.1.4.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.5.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.6.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.7.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.8.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.9.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.10.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.11.1 = Counter32: 1 (fgAvFTPVirusDetected)
iso.3.6.1.4.1.12356.101.8.2.1.1.12.1 = Counter32: 1 (fgAvFTPVirusBlocked)
iso.3.6.1.4.1.12356.101.8.2.1.1.13.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.14.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.15.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.16.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.17.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.18.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.19.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.20.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.21.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.22.1 = Counter32: 0
```

## 8. Optionally, reset the antivirus statistics to zero:

```
diagnose ips av stats clear
```

## CIFS support

File filtering and antivirus scanning for proxy-based inspection on Common Internet File System (CIFS) traffic is supported.

File filtering for CIFS is performed by inspecting the first 4 KB of the file to identify the file's magic number. If a match occurs, CIFS file filtering prevents the CIFS command that contains that file from running.

The CIFS security profile handles the configuration of file filtering on CIFS. The antivirus profile handles the antivirus configuration for CIFS scanning.

For a CIFS profile to be available for assignment in a policy, the policy must use proxy inspection mode. See [Proxy mode inspection on page 1086](#) for details.

The following are not supported by CIFS scanning in proxy inspection mode:

- File types and infections within archive files cannot be detected.
- Oversized files cannot be detected.
- Special condition archive files (encrypted, corrupted, mailbomb, and so on) marked by the antivirus engine are blocked automatically.

## Supported file types

File filter supports the following file types:

File Type Name	Description
7z	Match 7-zip files
arj	Match arj compressed files
cab	Match Windows cab files
lzh	Match lzh compressed files
rar	Match rar archives
tar	Match tar files
zip	Match zip files
bzip	Match bzip files
gzip	Match gzip files
bzip2	Match bzip2 files
xz	Match xz files
bat	Match Windows batch files
msc	Match msc files
uue	Match uue files
mime	Match mime files
base64	Match base64 files
binhex	Match binhex files
bin	Match bin files
elf	Match elf files
exe	Match Windows executable files
hta	Match hta files
html	Match html files
jad	Match jad files
class	Match class files
cod	Match cod files

File Type Name	Description
javascript	Match javascript files
msoffice	Match MS-Office files. For example, doc, xls, ppt, and so on.
msofficex	Match MS-Office XML files. For example, docx, xlsx, pptx, and so on.
fsg	Match fsg files
upx	Match upx files
petite	Match petite files
aspack	Match aspack files
prc	Match prc files
sis	Match sis files
hlp	Match Windows help files
activemime	Match activemime files
jpeg	Match jpeg files
gif	Match gif files
tiff	Match tiff files
png	Match png files
bmp	Match bmp files
unknown	Match unknown files
mpeg	Match mpeg files
mov	Match mov files
mp3	Match mp3 files
wma	Match wma files
wav	Match wav files
pdf	Match pdf files
avi	Match avi files
rm	Match rm files
torrent	Match torrent files
msi	Match Windows Installer msi bzip files
mach-o	Match Mach object files
dmg	Match Apple disk image files
.net	Match .NET files

File Type Name	Description
xar	Match xar archive files
chm	Match Windows compiled HTML help files
iso	Match ISO archive files
crx	Match Chrome extension files

## Configure file-type filtering and antivirus scanning on CIFS traffic

To configure file-type filtering and antivirus scanning on CIFS traffic:

1. [Configure a CIFS domain controller on page 921](#)
2. [Configure a CIFS profile on page 921](#)
3. [Configure an antivirus profile on page 923](#)

### Configure a CIFS domain controller

The domain controller must be configured when CIFS traffic is encrypted, like SMB 3.0 traffic. The configuration tells the FortiGate the network location of the domain controller and the superuser credentials.

To configure the CIFS domain controller:

```
config cifs domain-controller
 edit "DOMAIN"
 set domain-name "EXAMPLE.COM"
 set username "admin-super"
 set password "*****"
 set ip 172.16.201.40
 next
end
```

### Configure a CIFS profile

To create a CIFS profile, configure the server credential type and add file filter entries.

#### Set the CIFS server credential type

The CIFS server credential type can be `none`, `credential-replication`, or `credential-keytab`.

##### **none**

The CIFS profile assumes the CIFS traffic is unencrypted (used with SMB 2.0). This is the default value.

```
config cifs profile
 edit "cifs"
 set server-credential-type none
 next
end
```

## credential-replication

To decrypt CIFS traffic, FortiOS obtains the session key from the domain controller by logging in to the superuser account. The domain controller must be configured.

```
config cifs profile
 edit "cifs"
 set server-credential-type credential-replication
 set domain-controller "DOMAIN"
 next
end
```

Variable	Description
domain-controller <string>	The previously configured domain to decrypt CIFS traffic for.

## credential-keytab

To decrypt CIFS traffic, FortiOS uses a series of keytab values. This method is used when the SMB connection is authenticated by Kerberos. Keytab entries must be configured, and are stored in FortiOS in plaintext.

```
config cifs profile
 edit "cifs"
 set server-credential-type credential-keytab
 config server-keytab
 edit "keytab1"
 set keytab
 "BQIAAABFAAEAC0VYQU1QTEUuQ09NAAdleGFtcGx1AAAAVUmAlwBABIAILdV5P6NXT8RrTvapcMJQxDYCjRQid0Bzxh
 wS9h0VgyM"
 next
 end
 next
end
```

Variable	Description
keytab <keytab>	Base64 encoded keytab file containing the credentials of the server.

## Configure CIFS profile file filtering

Multiple file filter entries can be added to a profile.

### To configure a file filter entry in a CIFS profile:

```
config cifs profile
 edit "cifs"
 config file-filter
 set status {enable | disable}
 set log {enable | disable}
 config entries
 edit <filter>
 set comment <string>
 set action {log | block}
 set direction {incoming | outgoing | any}
 set file-type <file_type>
 next
 next
 end
 next
end
```



```

 next
 end
 end
 next
end

```

Variable	Description
status {enable   disable}	Enable/disable file filter (default = enable).
log {enable   disable}	Enable/disable file filter logging (default = enable).
comment <string>	A brief comment describing the entry.
action {log   block}	The action to take for matched files: <ul style="list-style-type: none"> <li>log: Allow the content and write a log message (default).</li> <li>block: Block the content and write a log message.</li> </ul>
direction {incoming   outgoing   any}	Match files transmitted in the session's originating ( <i>incoming</i> ) and/or reply ( <i>outgoing</i> ) direction (default = any).
file-type <file_type>	The file types to be matched (default = none). See <a href="#">Supported file types on page 919</a> for details.

## Configure an antivirus profile

The antivirus profile handles the antivirus configuration for CIFS scanning.

### To configure an antivirus profile:

```

config antivirus profile
 edit "av"
 ...
 config cifs
 set options {scan avmonitor quarantine}
 set archive-block {encrypted corrupted partiallycorrupted multipart nested
mailbomb fileslimit timeout unhandled}
 set archive-log {encrypted corrupted partiallycorrupted multipart nested
mailbomb fileslimit timeout unhandled}
 set emulator {enable | disable}
 set outbreak-prevention {disabled | files | full-archive}
 end
 next
end

```

Variable	Description
options {scan avmonitor quarantine}	Enable/disable CIFS antivirus scanning, monitoring, and quarantine.
archive-block {encrypted corrupted partiallycorrupted multipart nested mailbomb fileslimit timeout unhandled}	Select the archive types to block: <ul style="list-style-type: none"> <li>encrypted: Block encrypted archives.</li> <li>corrupted: Block corrupted archives.</li> <li>partiallycorrupted: Block partially corrupted archives.</li> <li>multipart: Block multipart archives.</li> </ul>

Variable	Description
	<ul style="list-style-type: none"> <li>nested: Block nested archives.</li> <li>mailbomb: Block mail bomb archives.</li> <li>fileslimit: Block exceeded archive files limit.</li> <li>timeout: Block scan timeout.</li> <li>unhandled: Block archives that FortiOS cannot open.</li> </ul>
archive-log {encrypted corrupted partiallycorrupted multipart nested mailbomb fileslimit timeout unhandled}	Select the archive types to log: <ul style="list-style-type: none"> <li>encrypted: Log encrypted archives.</li> <li>corrupted: Log corrupted archives.</li> <li>partiallycorrupted: Log partially corrupted archives.</li> <li>multipart: Log multipart archives.</li> <li>nested: Log nested archives.</li> <li>mailbomb: Log mail bomb archives.</li> <li>fileslimit: Log exceeded archive files limit.</li> <li>timeout: Log scan timeout.</li> <li>unhandled: Log archives that FortiOS cannot open.</li> </ul>
emulator {enable   disable}	Enable/disable the virus emulator (default = enable).
outbreak-prevention {disabled   files   full-archive}	Enable the virus outbreak prevention service: <ul style="list-style-type: none"> <li>disabled: Disabled (default).</li> <li>files: Analyze files as sent, not the content of archives.</li> <li>full-archive: Analyze files, including the content of archives.</li> </ul>

## Log examples

File-type detection events generated by CIFS profiles are logged in the `utm-cifs` log category. Antivirus detection over the CIFS protocol generates logs in the `utm-virus` category. See the [FortiOS Log Message Reference](#) for more information.

### Logs generated by CIFS profile file filter:

```
date=2019-03-28 time=10:39:19 logid="1800063001" type="utm" subtype="cifs" eventtype="cifs-filefilter" level="notice" vd="vdom1" eventtime=1553794757 msg="File was detected by file filter." direction="incoming" action="passthrough" service="CIFS" srcip=10.1.100.11 dstip=172.16.200.44 srcport=33372 dstport=445 srcintf="wan2" srcintfrole="wan" dstintf="wan1" dstintfrole="wan" policyid=1 proto=16 profile="cifs" filesize="1154" filename="virus\\test.png" filtername="2" filetype="png"
```

```
date=2019-03-28 time=10:39:12 logid="1800063001" type="utm" subtype="cifs" eventtype="cifs-filefilter" level="notice" vd="vdom1" eventtime=1553794751 msg="File was detected by file filter." direction="incoming" action="passthrough" service="CIFS" srcip=10.1.100.11 dstip=172.16.200.44 srcport=33370 dstport=445 srcintf="wan2" srcintfrole="wan" dstintf="wan1" dstintfrole="wan" policyid=1 proto=16 profile="cifs" filesize="81975" filename="virus\\screen.png" filtername="2" filetype="png"
```

```
date=2019-03-28 time=10:33:55 logid="1800063000" type="utm" subtype="cifs" eventtype="cifs-filefilter" level="warning" vd="vdom1" eventtime=1553794434 msg="File was blocked by file filter." direction="incoming" action="blocked" service="CIFS" srcip=10.1.100.11 dstip=172.16.200.44 srcport=33352 dstport=445 srcintf="wan2" srcintfrole="wan"
```

```
dstintf="wan1" dstintfrole="wan" policyid=1 proto=16 profile="cifs" filesize="28432"
filename="filetypes\\mpnotify.exe" filtername="3" filetype="exe"
```

```
date=2019-03-28 time=10:33:45 logid="1800063000" type="utm" subtype="cifs" eventtype="cifs-
filefilter" level="warning" vd="vdom1" eventtime=1553794424 msg="File was blocked by file
filter." direction="incoming" action="blocked" service="CIFS" srcip=10.1.100.11
dstip=172.16.200.44 srcport=33348 dstport=445 srcintf="wan2" srcintfrole="wan"
dstintf="wan1" dstintfrole="wan" policyid=1 proto=16 profile="cifs" filesize="96528"
filename="filetypes\\winmine.exe" filtername="3" filetype="exe"
```

### Logs generated by AV profile for infections detected over CIFS:

```
date=2019-04-09 time=15:19:02 logid="0204008202" type="utm" subtype="virus"
eventtype="outbreak-prevention" level="warning" vd="vdom1" eventtime=1554848342519005401
msg="Blocked by Virus Outbreak Prevention service." action="blocked" service="SMB"
sessionid=177 srcip=10.1.100.11 dstip=172.16.200.44 srcport=37444 dstport=445 srcintf="wan2"
srcintfrole="wan" dstintf="wan1" dstintfrole="wan" policyid=1 proto=6 direction="incoming"
filename="outbreak\\zhvo_test.com" quarskip="File-was-not-quarantined."
virus="503e99fe40ee120c45bc9a30835e7256fff3e46a" dtype="File Hash"
filehash="503e99fe40ee120c45bc9a30835e7256fff3e46a" filehashsrc="fortiguard" profile="av"
analyticssubmit="false" crscore=50 craction=2 crlevel="critical"
```

```
date=2019-04-09 time=15:18:59 logid="0211008192" type="utm" subtype="virus"
eventtype="infected" level="warning" vd="vdom1" eventtime=1554848339909808987 msg="File is
infected." action="blocked" service="SMB" sessionid=174 srcip=10.1.100.11
dstip=172.16.200.44 srcport=37442 dstport=445 srcintf="wan2" srcintfrole="wan"
dstintf="wan1" dstintfrole="wan" policyid=1 proto=6 direction="incoming"
filename="sample\\eicar.com" quarskip="File-was-not-quarantined." virus="EICAR_TEST_FILE"
dtype="Virus" ref="http://www.fortinet.com/ve?vn=EICAR_TEST_FILE" virusid=2172 profile="av"
analyticscksum="275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f"
analyticssubmit="false" crscore=50 craction=2 crlevel="critical"
```

## Databases

The antivirus scanning engine uses a virus signatures database to record the unique attributes of each infection. The antivirus scan searches for these signatures and when one is discovered, the FortiGate unit determines if the file is infected and takes action.

All FortiGate units have the normal antivirus signature database. The FortiGate 300D is the lowest model that supports the extreme database. All VMs support the extreme database. Some models have additional databases that you can use. The database that you use depends on your network and security needs.

<b>Normal</b>	Includes currently spreading viruses, as determined by the FortiGuard Global Security Research Team. These viruses are the greatest threat.
<b>Extended</b>	Includes the normal database, as well as recent viruses that are no longer active. This is the default setting. These viruses may have been spreading within the last year but have since nearly or completely disappeared.
<b>Extreme</b>	Includes the extended database, as well as a large collection of zoo viruses. These are viruses that have not spread in a long time and are largely dormant. Some zoo viruses might rely on operating systems and hardware that are no longer widely used.

The extended virus definitions database is the default setting and provides comprehensive antivirus protection. This coverage comes at a cost because more processing requires additional resources.

**To change the antivirus database:**

```
config antivirus settings
 set default-db {normal | extended | extreme}
end
```

## Using FortiSandbox appliance with antivirus

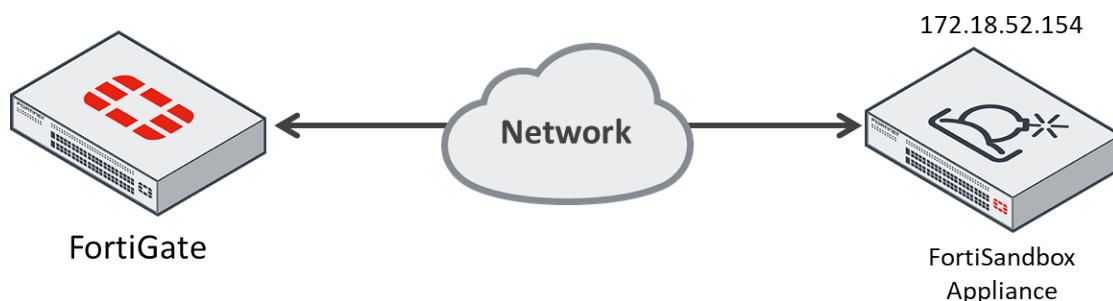
Antivirus can use FortiSandbox to supplement its detection capabilities. In real-world situations, networks are always under the threat of zero-day attacks.

Antivirus can submit potential zero-day viruses to FortiSandbox for inspection. Based on FortiSandbox's analysis, the FortiGate can supplement its own antivirus database with FortiSandbox's database to detect files determined as malicious or risky by FortiSandbox. This helps FortiGate antivirus detect zero-day viruses and malware whose signatures are not found in the FortiGate antivirus database.

### Support and limitations

- FortiSandbox can be used with antivirus in both proxy-based and flow-based inspection modes.
- Default scan mode antivirus cannot submit only suspicious files to FortiSandbox. It can only do the following:
  - Submit every file to FortiSandbox for inspection.
  - Not submit anything.
- With FortiSandbox enabled, legacy scan mode antivirus can do the following:
  - Submit only suspicious files to FortiSandbox for inspection.
  - Submit every file to FortiSandbox for inspection.
  - Not submit anything.

### Network topology example



### Configuring the feature

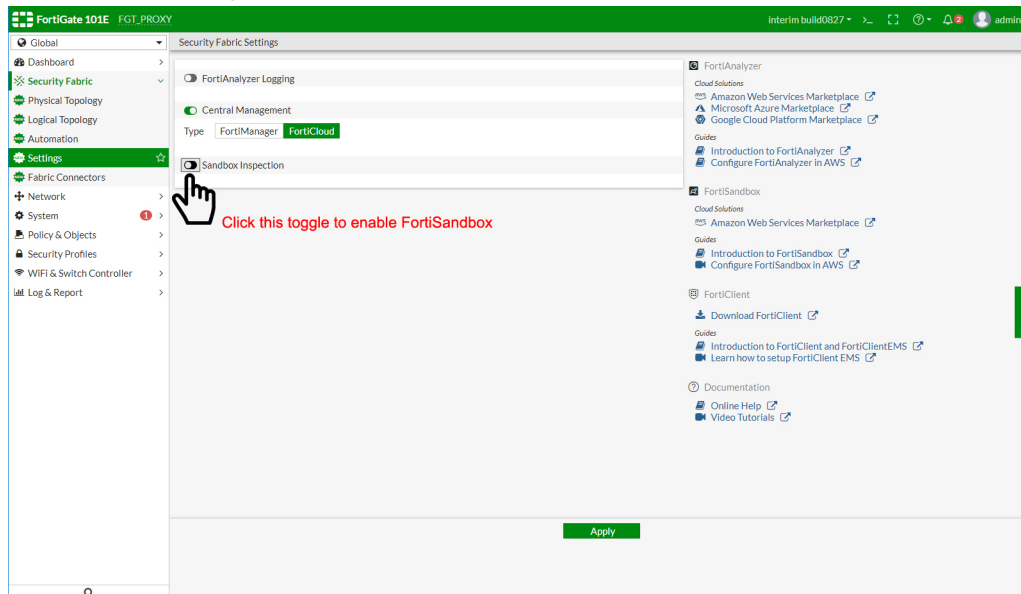
To configure antivirus to work with an external block list, the following steps are required:

1. [Enable FortiSandbox on the FortiGate.](#)
2. [Authorize FortiGate on the FortiSandbox.](#)

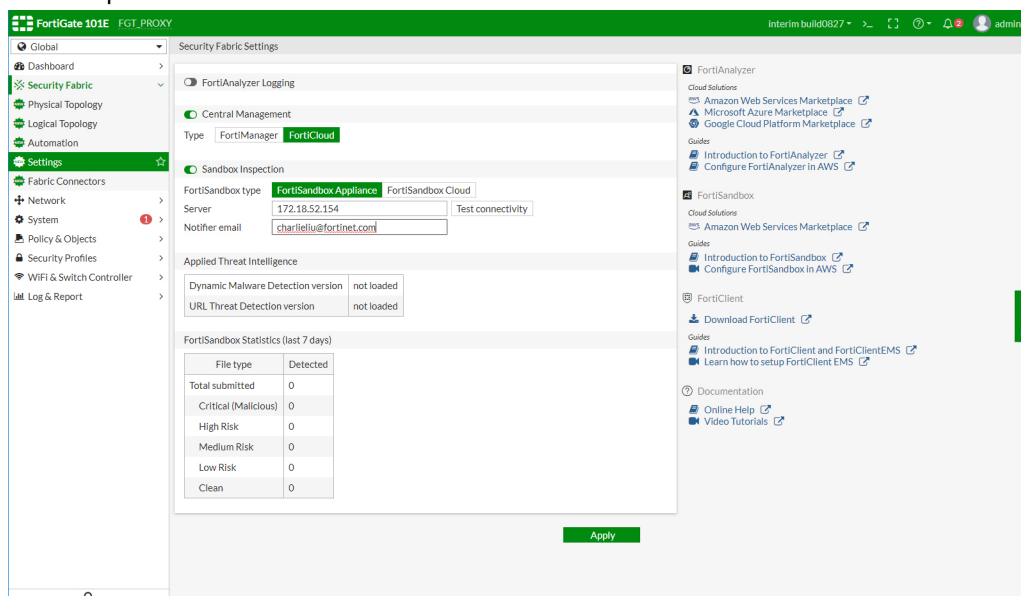
3. Enable FortiSandbox inspection.
4. Enable use of the FortiSandbox database.

To enable FortiSandbox on the FortiGate:

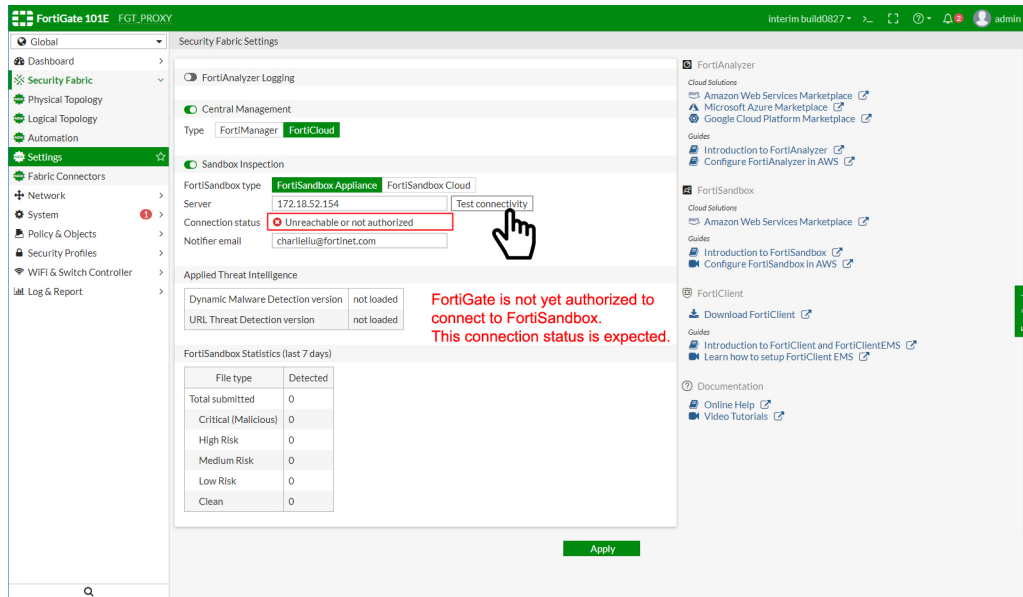
1. Go to *Global > Security Fabric > Settings*.
2. Enable *Sandbox Inspection*.



3. Enter the IP address of the FortiSandbox.
4. Add an optional *Notifier email* if desired.



5. At this point, selecting *Test connectivity* will return an unreachable status. This is expected, because the FortiGate is not yet authorized by the FortiSandbox.



6. Click *Apply* to save the settings.

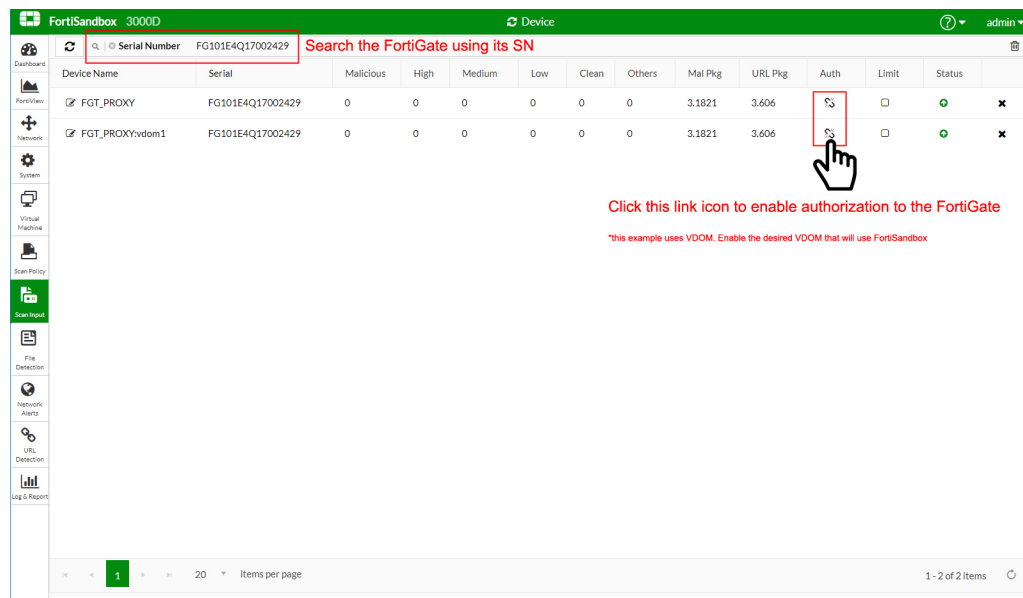
To authorize FortiGate on the FortiSandbox:

1. In the FortiSandbox Appliance GUI, go to *Scan Input > Device*.

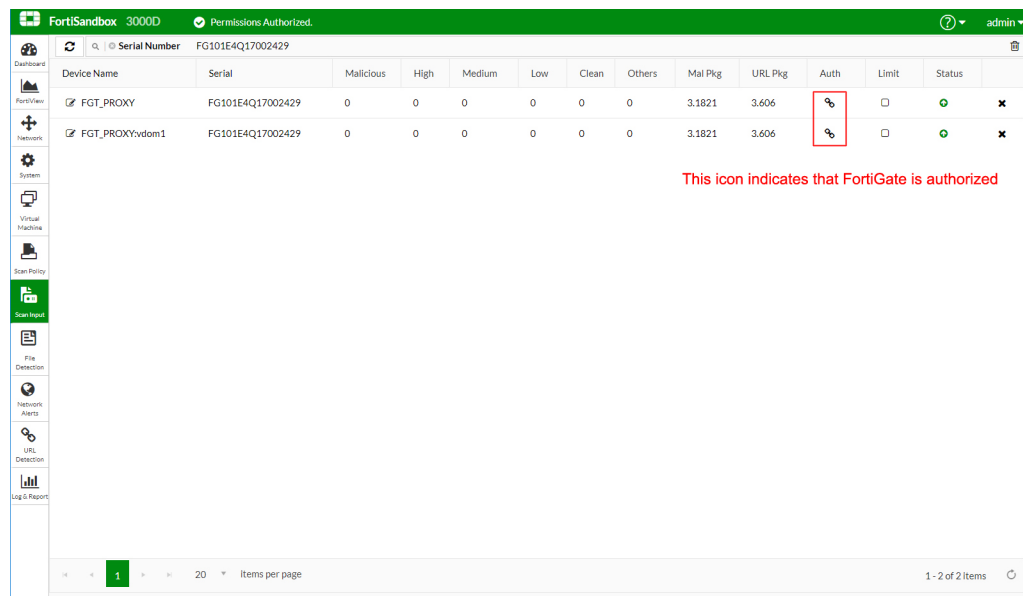
FortiSandbox 3000D												Device	admin
What are you looking for?													
Dashboard	FortiView	Network	System	Virtual Machine	Scan Policy	Scan Input	File On-Demand	URL On-Demand	Job Queue	Sniffer	Device	FortiClient	Adapter
Network Share	Quarantine	Malware Package	URL Package	File Detection	Network Alerts	URL Detection	Log & Report						
Device Name	Serial	Malicious	High	Medium	Low	Clean	Others	Mal Pkg	URL Pkg	Auth	Limit		
FG1	FG100D3G12804561	0	0	0	0	0	0	N/A	N/A	🔗	□		
FGT301E-WANOPT-S	FG3H1E5818901558	0	0	0	0	0	0	N/A	N/A	🔗	□		
William-WifiLab-FGT-300D	FGT5HD3915803287	0	0	0	0	0	0	N/A	N/A	🔗	□		
Starr-lab-130-FGT200D-PFW	FG200D3916803286	0	0	0	0	0	0	N/A	N/A	🔗	□		
leolu_PFW_FGT100D	FG100D3G12811597	0	0	0	0	0	0	N/A	N/A	🔗	□		
Noble-Lab-PRFW-FortiGate-200E	FG200E4Q17911664	0	0	0	0	0	0	N/A	N/A	🔗	□		
Dave-Lab-PFW-FortiGate-100D	FG100D3G14827006	0	0	0	0	0	0	N/A	N/A	🔗	□		
William-WifiLab-FGT-301E	FG3H1E5818900737	0	0	0	0	0	0	N/A	N/A	🔗	□		
FW_QA1	FG3K2D3Z16800032	0	0	0	0	2517	0	3.1834	3.614	🔗	□		
FW_QA1:root	FG3K2D3Z16800032	0	0	0	0	2517	0	3.1834	3.614	🔗	□		
Chuxin_PFW_FGT92D	FGT92D3G16001001	0	0	0	0	0	0	N/A	N/A	🔗	□		
Yong_PFW_1	FGT90D3Z14016614	0	0	0	0	0	0	N/A	N/A	🔗	□		
Bruce-lxia_FGT501E	FG5H1E5818900015	0	0	0	0	0	0	N/A	N/A	🔗	□		
ZachWang_lab_PFW	FG100D3G12806923	0	0	0	0	0	0	N/A	N/A	🔗	□		
yuzhu-desktop-	FG100D3G12806923	0	0	0	0	0	0	N/A	N/A	🔗	□		

2. Use the FortiGate serial number to quickly locate the desired FortiGate and select the *link* icon to authorize the FortiGate.

3. Enable the desired VDOM in the same manner.

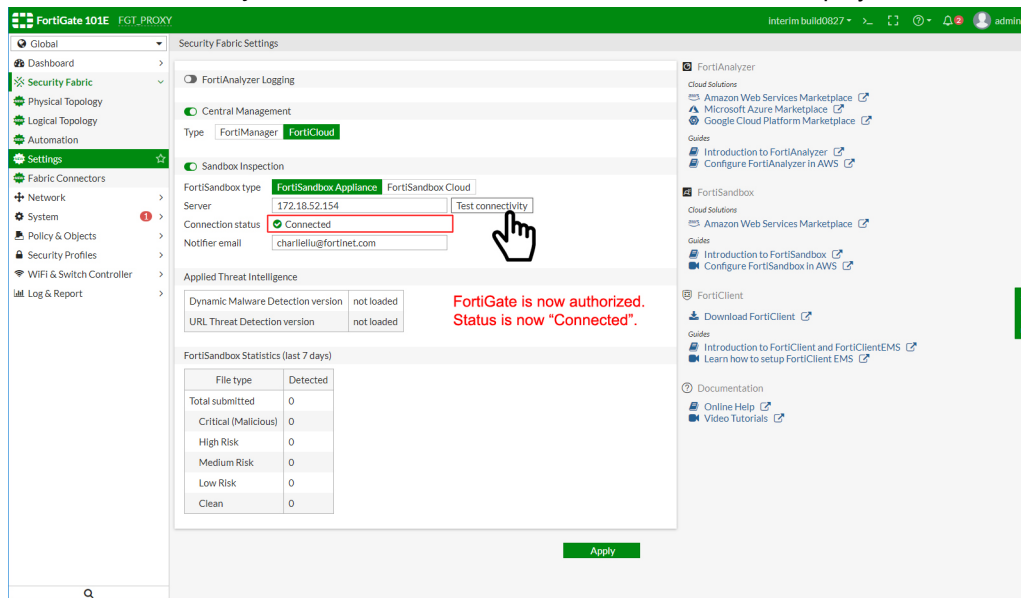


4. The *link* icon changes from an open to closed link. This indicates that the FortiSandbox has authorized this FortiGate.

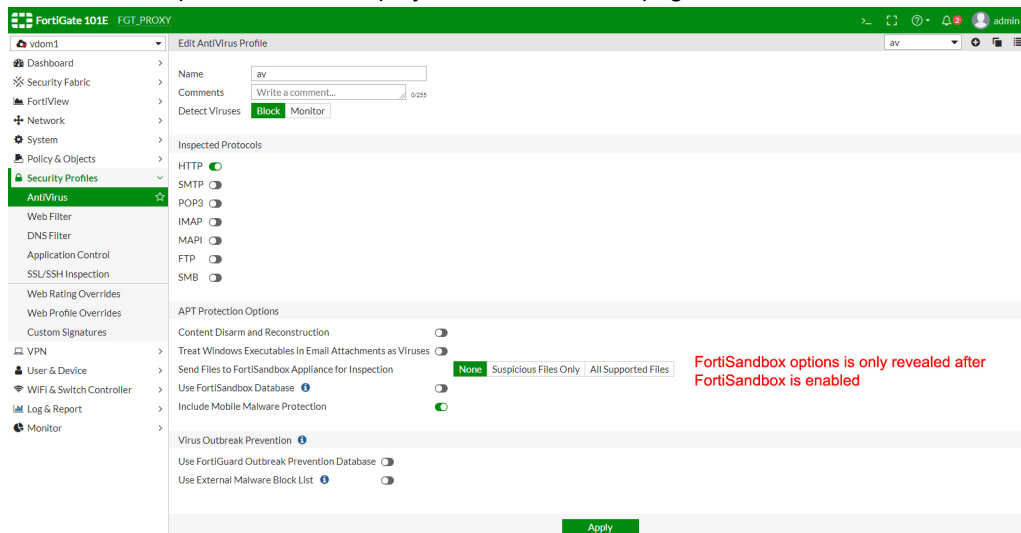


5. In the FortiGate GUI, go to *Global > Security Fabric > Settings*.

6. Click *Test connectivity*. The FortiGate is now authorized and the status displays as *Connected*.



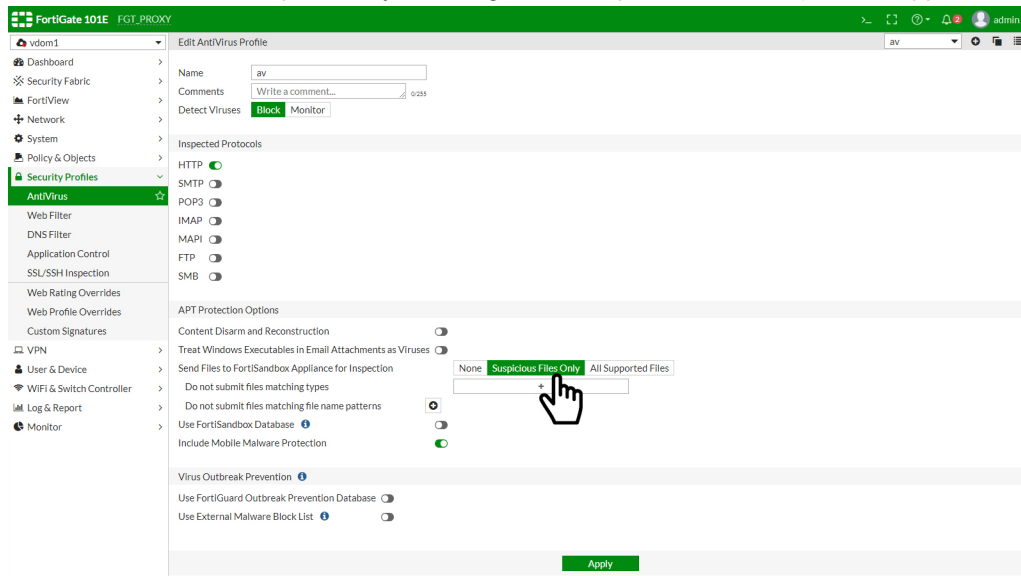
7. FortiSandbox options are now displayed in the AV Profile page.



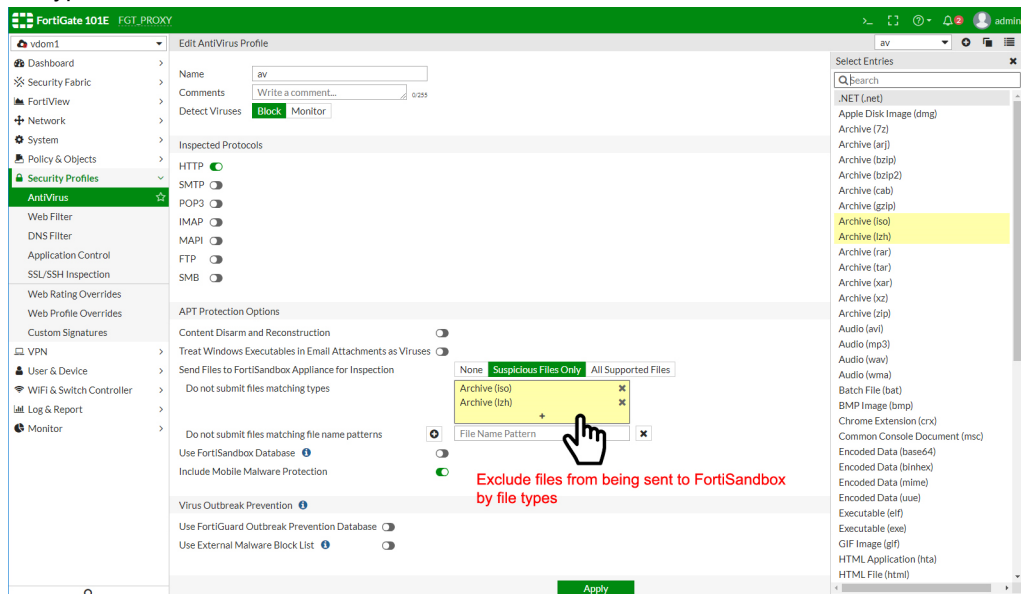


## To enable FortiSandbox inspection:

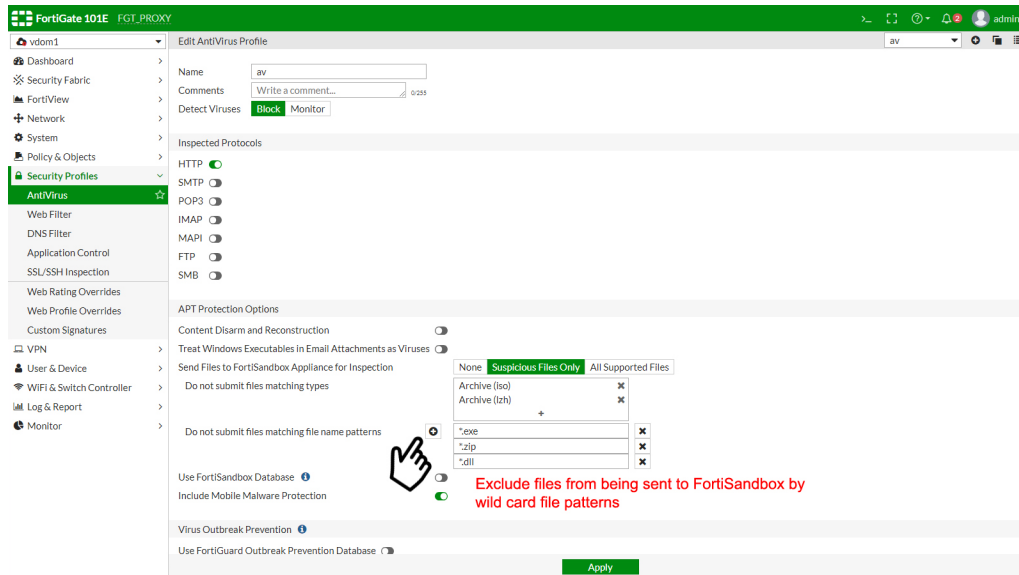
1. Go to *Security Profiles > AntiVirus*.
2. Enable FortiSandbox inspection by selecting either *Suspicious Files Only* or *All Supported Files*.



3. Files can be excluded from being sent to FortiSandbox based on their file types by choosing from a list of supported file types.



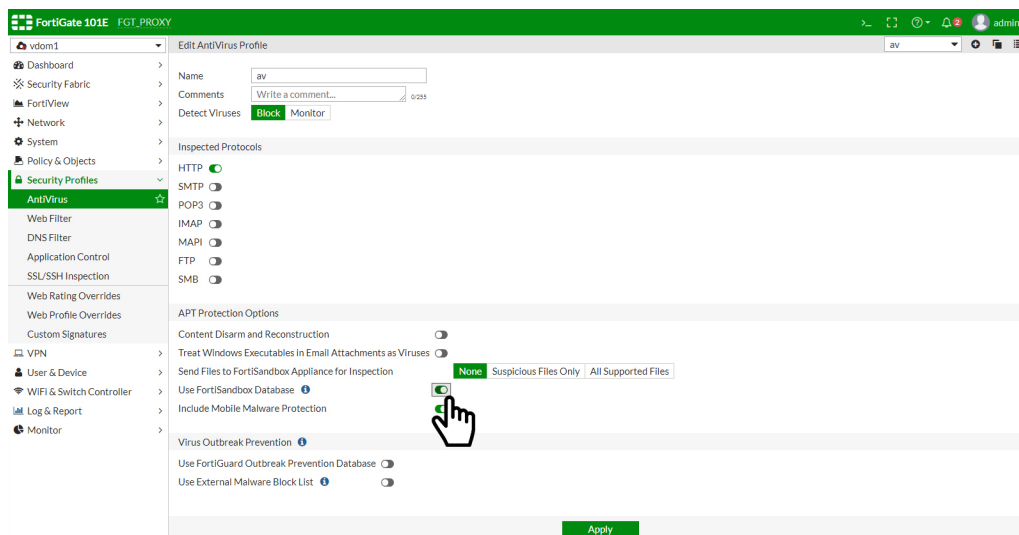
4. Files can also be excluded from being sent to FortiSandbox by using wildcard patterns.



5. Click *Apply*.

To enable use of the FortiSandbox database:

1. Go to *Security Profiles > AntiVirus*
2. Enable *Use FortiSandbox Database*.



3. Click *Apply*.

## Diagnostics and Debugging

### Debug on the FortiGate side

- Update daemon:

```
FGT_PROXY (global) # diagnose debug application quarantined -1
FGT_PROXY (global) # diagnose debug enable

quar_req_fsa_file()-890: fsa ext list new_version (1547781904)
quar_fsb_handle_quar()-1439: added a req-6 to fortisandbox-fsb5, vfid=1, oftp-name=[].
__quar_start_connection()-908: start server fortisandbox-fsb5-172.18.52.154 in vdom-1
[103] __ssl_cert_ctx_load: Added cert /etc/cert/factory/root_Fortinet_Factory.cer, root
ca Fortinet_CA, idx 0 (default)
[551] ssl_ctx_create_new_ex: SSL CTX is created
[578] ssl_new: SSL object is created
upd_cfg_extract_av_db_version[378]-version=06002000AVDB00201-00066.01026-1901301530
upd_cfg_extract_ids_db_version[437]-version=06002000NIDS02403-00014.00537-1901300043
upd_cfg_extract_ids_db_version[437]-version=06002000APDB00103-00006.00741-1512010230
upd_cfg_extract_ids_db_version[437]-version=06002000ISDB00103-00014.00537-1901300043
upd_cfg_extract_ibdb_botnet_db_version[523]-version=06002000IBDB00101-00004.00401-
1901281000
upd_cfg_extract_av_db_version[378]-version=06002000AVDB00201-00066.01026-1901301530
upd_cfg_extract_ids_db_version[437]-version=06002000NIDS02403-00014.00537-1901300043
upd_cfg_extract_ids_db_version[437]-version=06002000APDB00103-00006.00741-1512010230
upd_cfg_extract_ids_db_version[437]-version=06002000ISDB00103-00014.00537-1901300043
upd_cfg_extract_ibdb_botnet_db_version[523]-version=06002000IBDB00101-00004.00401-
1901281000
upd_cfg_extract_av_db_version[378]-version=06002000AVDB00201-00066.01026-1901301530
upd_cfg_extract_ids_db_version[437]-version=06002000NIDS02403-00014.00537-1901300043
upd_cfg_extract_ids_db_version[437]-version=06002000APDB00103-00006.00741-1512010230
upd_cfg_extract_ids_db_version[437]-version=06002000ISDB00103-00014.00537-1901300043
upd_cfg_extract_ibdb_botnet_db_version[523]-version=06002000IBDB00101-00004.00401-
1901281000
upd_cfg_extract_av_db_version[378]-version=06002000AVDB00201-00066.01026-1901301530
upd_cfg_extract_ids_db_version[437]-version=06002000NIDS02403-00014.00537-1901300043
upd_cfg_extract_ids_db_version[437]-version=06002000APDB00103-00006.00741-1512010230
upd_cfg_extract_ids_db_version[437]-version=06002000ISDB00103-00014.00537-1901300043
upd_cfg_extract_ibdb_botnet_db_version[523]-version=06002000IBDB00101-00004.00401-
1901281000
upd_cfg_extract_av_db_version[378]-version=06002000AVDB00201-00066.01026-1901301530
upd_cfg_extract_ids_db_version[437]-version=06002000NIDS02403-00014.00537-1901300043
upd_cfg_extract_ids_db_version[437]-version=06002000APDB00103-00006.00741-1512010230
upd_cfg_extract_ids_db_version[437]-version=06002000ISDB00103-00014.00537-1901300043
upd_cfg_extract_ibdb_botnet_db_version[523]-version=06002000IBDB00101-00004.00401-
1901281000
quar_remote_recv_send()-731: dev=fortisandbox-fsb2 xfer-status=0
__quar_build_pkt()-408: build req(id=337, type=4) for vdom-vdom1, len=99, oftp_name=
__quar_send()-470: dev buffer -- pos=0, len=99
quar_remote_send()-520: req(id=337, type=4) read response, dev=fortisandbox-fsb2, xfer_
status=1, buflen=12
quar_remote_recv_send()-770: dev=fortisandbox-fsb2, oevent=4, nevent=1, xfer-status=1
quar_remote_recv_send()-731: dev=fortisandbox-fsb3 xfer-status=0
__quar_build_pkt()-408: build req(id=338, type=6) for vdom-vdom1, len=93, oftp_name=
__quar_send()-470: dev buffer -- pos=0, len=93
quar_remote_send()-520: req(id=338, type=6) read response, dev=fortisandbox-fsb3, xfer_
```

```

status=1, buflen=12
quar_remote_recv_send()-770: dev=fortisandbox-fsb3, oevent=4, nevent=1, xfer-status=1
quar_remote_recv_send()-731: dev=fortisandbox-fsb5 xfer-status=0
__quar_build_pkt()-408: build req(id=340, type=6) for vdom-vdom1, len=93, oftp_name=
__quar_send()-470: dev buffer -- pos=0, len=93
quar_remote_send()-520: req(id=340, type=6) read response, dev=fortisandbox-fsb5, xfer_
status=1, buflen=12
quar_remote_recv_send()-770: dev=fortisandbox-fsb5, oevent=4, nevent=1, xfer-status=1
quar_remote_recv_send()-731: dev=fortisandbox-fsb2 xfer-status=1
quar_remote_recv()-662: dev(fortisandbox-fsb2) received a packet: len=69, type=1
quar_remote_recv()-718: file-[337] is accepted by server(fortisandbox-fsb2).
quar_put_job_req()-332: Job 337 deleted
quar_remote_recv_send()-731: dev=fortisandbox-fsb4 xfer-status=0
__quar_build_pkt()-408: build req(id=339, type=6) for vdom-vdom1, len=93, oftp_name=
__quar_send()-470: dev buffer -- pos=0, len=93
quar_remote_send()-520: req(id=339, type=6) read response, dev=fortisandbox-fsb4, xfer_
status=1, buflen=12
quar_remote_recv_send()-770: dev=fortisandbox-fsb4, oevent=4, nevent=1, xfer-status=1
quar_remote_recv_send()-731: dev=fortisandbox-fsb1 xfer-status=0
__quar_build_pkt()-408: build req(id=336, type=4) for vdom-root, len=98, oftp_name=
__quar_send()-470: dev buffer -- pos=0, len=98
...
__get_analytics_stats()-19: Received an ANALYTICS_STATS request, vfid: 0
__quar_req_handler()-127: Request 0 was handled successfully
__get_analytics_stats()-19: Received an ANALYTICS_STATS request, vfid: 0
__quar_req_handler()-127: Request 0 was handled successfully
__get_analytics_stats()-19: Received an ANALYTICS_STATS request, vfid: 0
__quar_req_handler()-127: Request 0 was handled successfully
__get_analytics_stats()-19: Received an ANALYTICS_STATS request, vfid: 0
__quar_req_handler()-127: Request 0 was handled successfully
quar_fsb_handle_quar()-1439: added a req-6 to fortisandbox-fsb1, vfid=1, oftp-name=[].
__quar_start_connection()-908: start server fortisandbox-fsb1-172.18.52.154 in vdom-1
[103] __ssl_cert_ctx_load: Added cert /etc/cert/factory/root_Fortinet_Factory.cer, root
ca Fortinet_CA, idx 0 (default)
[551] ssl_ctx_create_new_ex: SSL CTX is created
[578] ssl_new: SSL object is created
upd_cfg_extract_av_db_version[378]-version=06002000AVDB00201-00066.01026-1901301530
upd_cfg_extract_ids_db_version[437]-version=06002000NIDS02403-00014.00537-1901300043
upd_cfg_extract_ids_db_version[437]-version=06002000APDB00103-00006.00741-1512010230
upd_cfg_extract_ids_db_version[437]-version=06002000ISDB00103-00014.00537-1901300043
upd_cfg_extract_ibdb_botnet_db_version[523]-version=06002000IBDB00101-00004.00401-
1901281000
quar_remote_recv_send()-731: dev=fortisandbox-fsb1 xfer-status=0
__quar_build_pkt()-408: build req(id=2, type=6) for vdom-vdom1, len=93, oftp_name=
__quar_send()-470: dev buffer -- pos=0, len=93
quar_remote_send()-520: req(id=2, type=6) read response, dev=fortisandbox-fsb1, xfer_
status=1, buflen=12
quar_remote_recv_send()-770: dev=fortisandbox-fsb1, oevent=4, nevent=1, xfer-status=1
quar_remote_recv_send()-731: dev=fortisandbox-fsb1 xfer-status=1
quar_remote_recv()-662: dev(fortisandbox-fsb1) received a packet: len=767, type=1
quar_store_analytics_report()-590: Analytics-report return
file=/tmp/fsb/83bb2d9928b03a68b123730399b6b9365b5cc9a5a77f8aa007a6f1a499a13b18.json.gz,
buf_sz=735
quar_store_analytics_report()-597: The request
'83bb2d9928b03a68b123730399b6b9365b5cc9a5a77f8aa007a6f1a499a13b18' score is 1
quar_remote_recv()-718: file-[2] is accepted by server(fortisandbox-fsb1).

```

```

quar_put_job_req()-332: Job 2 deleted
quar_monitor_connection_func()-978: monitoring dev fortisandbox-fsb1
quar_monitor_connection_func()-978: monitoring dev fortisandbox-fsb1
__get_analytics_stats()-19: Received an ANALYTICS_STATS request, vfid: 0
__quar_req_handler()-127: Request 0 was handled successfully
__get_analytics_stats()-19: Received an ANALYTICS_STATS request, vfid: 0
__quar_req_handler()-127: Request 0 was handled successfully
quar_monitor_connection_func()-978: monitoring dev fortisandbox-fsb1
quar_stop_connection()-1006: close connection to server(fortisandbox-fsb1)
[193] __ssl_data_ctx_free: Done
[805] ssl_free: Done
[185] __ssl_cert_ctx_free: Done
[815] ssl_ctx_free: Done
[796] ssl_disconnect: Shutdown

```

- **Appliance FortiSandbox diagnostics:**

```

FGT_PROXY # config global
FGT_PROXY (global) # diagnose test application quarantined 1
Total remote&local devices: 8, any task full? 0
System have disk, vdom is enabled, mgmt=1, ha=2
xfer-fas is enabled: ips-archive dlp-archive, realtime=yes, taskfull=no
 addr=0.0.0.0/514, source-ip=0.0.0.0, keep-alive=no.
 ssl_opt=0, hmac_alg=0
 License=0, content_archive=0, arch_pause=0.

global-fas is disabled.
forticloud-fsb is disabled.
fortisandbox-fsb1 is enabled: analytics, realtime=yes, taskfull=no
 addr=172.18.52.154/514, source-ip=0.0.0.0, keep-alive=no.
 ssl_opt=3, hmac_alg=0
fortisandbox-fsb2 is enabled: analytics, realtime=yes, taskfull=no
 addr=172.18.52.154/514, source-ip=0.0.0.0, keep-alive=no.
 ssl_opt=3, hmac_alg=0
fortisandbox-fsb3 is enabled: analytics, realtime=yes, taskfull=no
 addr=172.18.52.154/514, source-ip=0.0.0.0, keep-alive=no.
 ssl_opt=3, hmac_alg=0
fortisandbox-fsb4 is enabled: analytics, realtime=yes, taskfull=no
 addr=172.18.52.154/514, source-ip=0.0.0.0, keep-alive=no.
 ssl_opt=3, hmac_alg=0
fortisandbox-fsb5 is enabled: analytics, realtime=yes, taskfull=no
 addr=172.18.52.154/514, source-ip=0.0.0.0, keep-alive=no.
 ssl_opt=3, hmac_alg=0
fortisandbox-fsb6 is enabled: analytics, realtime=yes, taskfull=no
 addr=172.18.52.154/514, source-ip=0.0.0.0, keep-alive=no.
 ssl_opt=3, hmac_alg=0
global-faz is disabled.
global-faz2 is disabled.
global-faz3 is disabled.

```

- **Checking FortiSandbox analysis statistics:**

```

FGT_PROXY (global) # diagnose test application quarantine 7
Total: 0

Statistics:
 vfid: 0, detected: 0, clean: 0, risk_low: 0, risk_med: 0, risk_high: 0, limit_
reached:0

```

```

vfid: 3, detected: 0, clean: 0, risk_low: 0, risk_med: 0, risk_high: 0, limit_
reached:0
vfid: 4, detected: 0, clean: 0, risk_low: 0, risk_med: 0, risk_high: 0, limit_
reached:0

```

```
FGT_PROXY (global) #
```

## Debug on the FortiSandbox side

- Appliance FortiSandbox OFTP debug:

```

diagnose-debug device FG101E4Q17002429

[2019/01/31 00:48:21] LOGIN->SUCCEED: Serial(FG101E4Q17002429), HOSTNAME(FGT_PROXY)
[2019/01/31 00:48:21] FG101E4Q17002429 VDOM: vdom1
[2019/01/31 00:48:21] FG101E4Q17002429 suspicious stats START_TIME: 1548290749
[2019/01/31 00:48:21] FG101E4Q17002429 suspicious stats END_TIME: 1548895549
[2019/01/31 00:48:21] FG101E4Q17002429 opd_data_len=37 clean=2 detected=2 risk_low=0
risk_med=0 risk_high=0 sus_limit=0
[2019/01/31 00:48:21] FG101E4Q17002429 ENTERING->HANDLE_SEND_FILE.
[2019/01/31 00:48:21] FG101E4Q17002429 ENTERING->HANDLE_SEND_FILE.
[2019/01/31 00:48:21] FG101E4Q17002429 INCOMING->FGT->VDOM: vdom1
[2019/01/31 00:48:21] FG101E4Q17002429 INCOMING->FGT->VDOM: vdom1
[2019/01/31 00:48:21] FG101E4Q17002429 INCOMING->IMG_VERSION: 6.2.0.0818
[2019/01/31 00:48:21] FG101E4Q17002429 INCOMING->IMG_VERSION: 6.2.0.0818
[2019/01/31 00:48:21] INCOMING->FGT: FG101E4Q17002429, VDOM: vdom1
[2019/01/31 00:48:21] INCOMING->FGT: FG101E4Q17002429, VDOM: vdom1
[2019/01/31 00:48:21] FG101E4Q17002429 INCOMING->TYPE: 0
[2019/01/31 00:48:21] FG101E4Q17002429 INCOMING->TYPE: 1
[2019/01/31 00:48:21] FG101E4Q17002429 INCOMING->VERSION: 3 . 1795
[2019/01/31 00:48:21] FG101E4Q17002429 INCOMING->VERSION: 3 . 595
[2019/01/31 00:48:21] FG101E4Q17002429 VDOM: root
[2019/01/31 00:48:21] FG101E4Q17002429 ENTERING->HANDLE_SEND_FILE.
[2019/01/31 00:48:21] FG101E4Q17002429 suspicious stats START_TIME: 1548290749
[2019/01/31 00:48:21] FG101E4Q17002429 INCOMING->FGT->VDOM: vdom1
[2019/01/31 00:48:21] FG101E4Q17002429 suspicious stats END_TIME: 1548895549
[2019/01/31 00:48:21] FG101E4Q17002429 INCOMING->IMG_VERSION: 6.2.0.0818
[2019/01/31 00:48:21] INCOMING->FGT: FG101E4Q17002429, VDOM: vdom1
[2019/01/31 00:48:21] FG101E4Q17002429 INCOMING->TYPE: 4
[2019/01/31 00:48:21] FG101E4Q17002429 opd_data_len=37 clean=0 detected=0 risk_low=0
risk_med=0 risk_high=0 sus_limit=0
[2019/01/31 00:48:22] FG101E4Q17002429 RETRIEVE->PKG: TYPE: av, ENTRY_VERSION: 1795,
PACKAGE_PATH: /Storage/malpkg/pkg/avsig/avsigrel_1795.pkg
[2019/01/31 00:48:22] FG101E4Q17002429 RETRIEVE->PKG: TYPE: url, ENTRY_VERSION: 595,
PACKAGE_PATH: /Storage/malpkg/pkg/url/urlrel_595.pkg.gz
[2019/01/31 00:48:29] LOGIN->SUCCEED: Serial(FG101E4Q17002429), HOSTNAME(FGT_PROXY)
[2019/01/31 00:48:32] LOGIN->SUCCEED: Serial(FG101E4Q17002429), HOSTNAME(FGT_PROXY)
[2019/01/31 00:48:59] LOGIN->SUCCEED: Serial(FG101E4Q17002429), HOSTNAME(FGT_PROXY)
[2019/01/31 00:49:03] LOGIN->SUCCEED: Serial(FG101E4Q17002429), HOSTNAME(FGT_PROXY)

```

## Using FortiSandbox Cloud with antivirus

## Feature overview

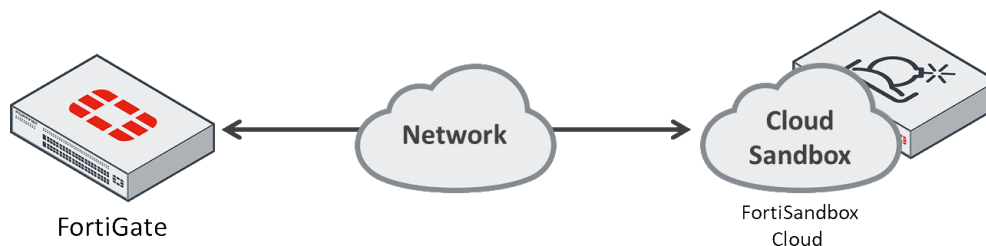
FortiSandbox Cloud allows users to take advantage of FortiSandbox features without having to purchase, operate, and maintain a physical appliance. It works the same way as the physical FortiSandbox appliance.

FortiSandbox Cloud allows you to control the region where your traffic is sent to for analysis. This allows you to meet your country's compliances regarding data storage locations.

## Support and limitations

- In FortiOS 6.2 and later, users do not require a FortiGate Cloud account to use FortiSandbox Cloud.
- Without a valid AVDB license, FortiGate devices are limited to 100 FortiGate Cloud submissions per day.
- Unlimited FortiGate Cloud submissions are allowed if the FortiGate has a valid AVDB license.
  - There is a limit on how many submissions are sent per minute.
  - The per-minute submission rate is based on the FortiGate model.
- FortiSandbox can be used with antivirus in both proxy-based and flow-based policy inspection modes.
- With FortiSandbox enabled, full scan mode antivirus can do the following:
  - Submit only suspicious files to FortiSandbox for inspection.
  - Submit every file to FortiSandbox for inspection.
  - Do not submit anything.
- Quick scan mode antivirus cannot submit suspicious files to FortiSandbox. It can only do the following:
  - Submit every file to FortiSandbox for inspection.
  - Do not submit anything.

## Network topology example



## Configuring the feature

To configure antivirus to work with an external block list, the following steps are required:

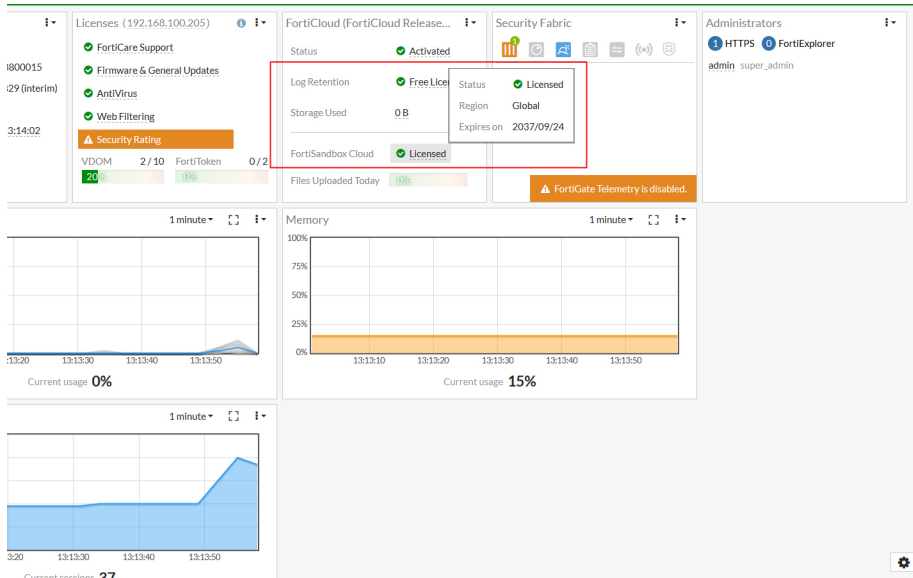
1. [Through FortiCare, register the FortiGate device and purchase a FortiGuard antivirus license](#)
2. [Enable FortiSandbox Cloud on the FortiGate](#)
3. [Enable FortiSandbox inspection](#)
4. [Enable the use of the FortiSandbox database](#)

### To obtain or renew an AVDB license:

1. Please see the video [How to Purchase or Renew FortiGuard Services](#) for FortiGuard antivirus license purchase instructions.

- Once a FortiGuard license has been purchased or activated, users will be provided with a paid FortiSandbox Cloud license.

- Go to *Global > Dashboard > Status* to view the FortiSandbox Cloud license indicator.



- Users can also view this indicator at *Global > System > FortiGuard*.

The screenshot shows the FortiGate System FortiGuard page. The 'FortiSandbox Cloud' license is listed as 'Licensed - expires on 2037/09/24'. A red box highlights the license details.

License Name	Status	Expires on
FortiSandbox Cloud	Licensed	2037/09/24

## To enable FortiSandbox Cloud on the FortiGate:

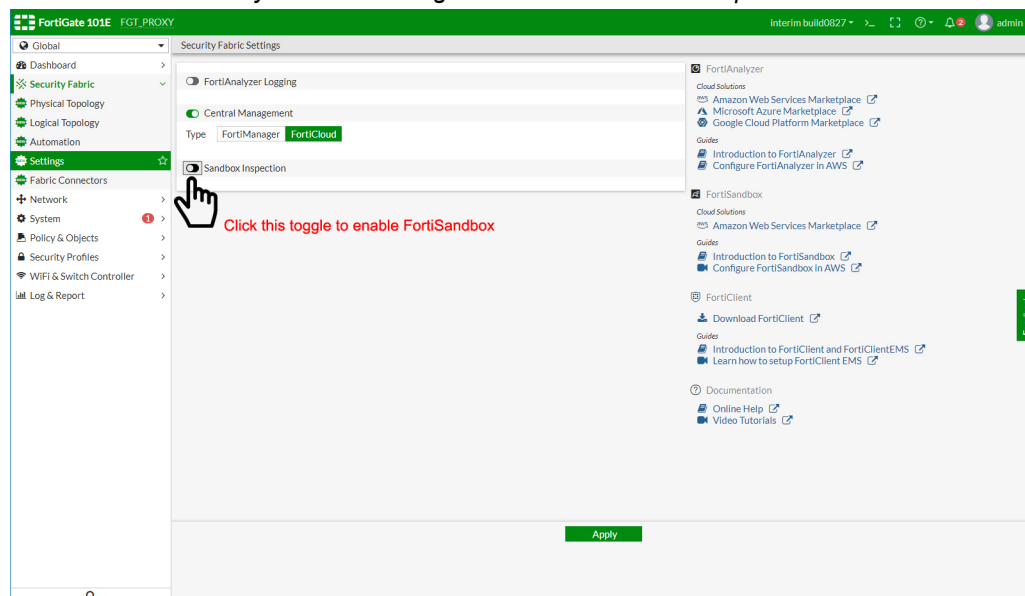
- Make the FortiSandbox Cloud feature visible:

```
config system global
 set gui-fortisandbox-cloud enable
end
```

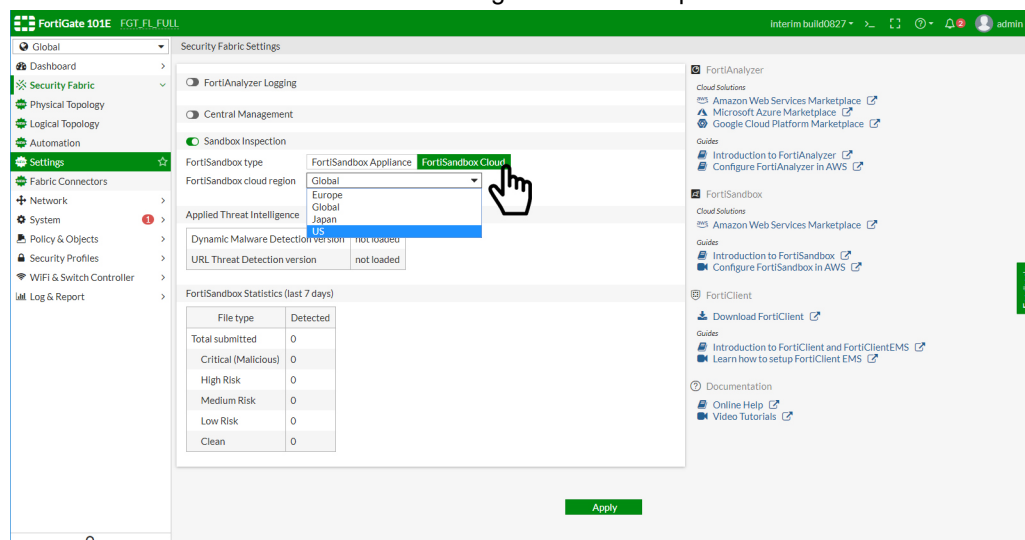
- Log out of FortiOS and log in again.



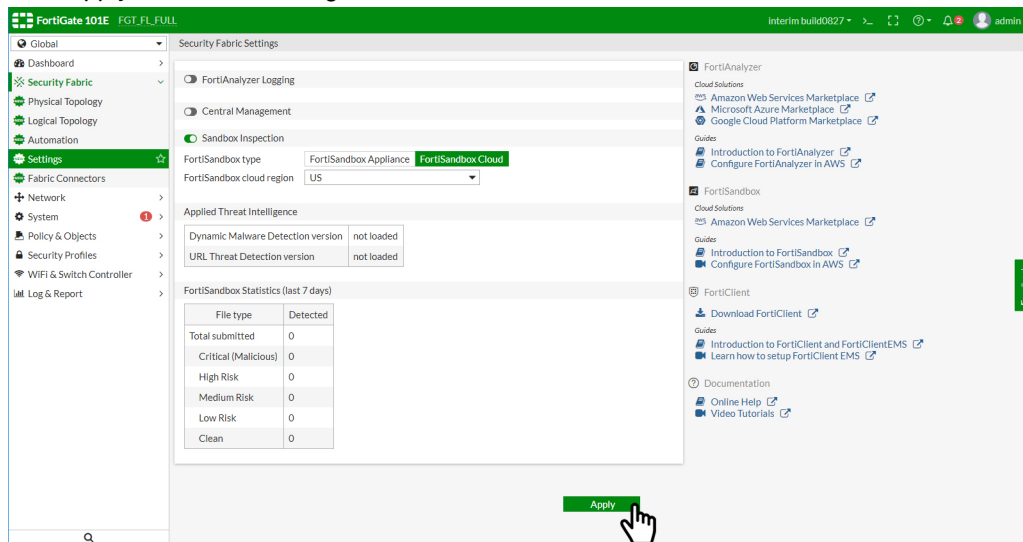
3. Go to *Global > Security Fabric > Settings* and enable *Sandbox Inspection*.



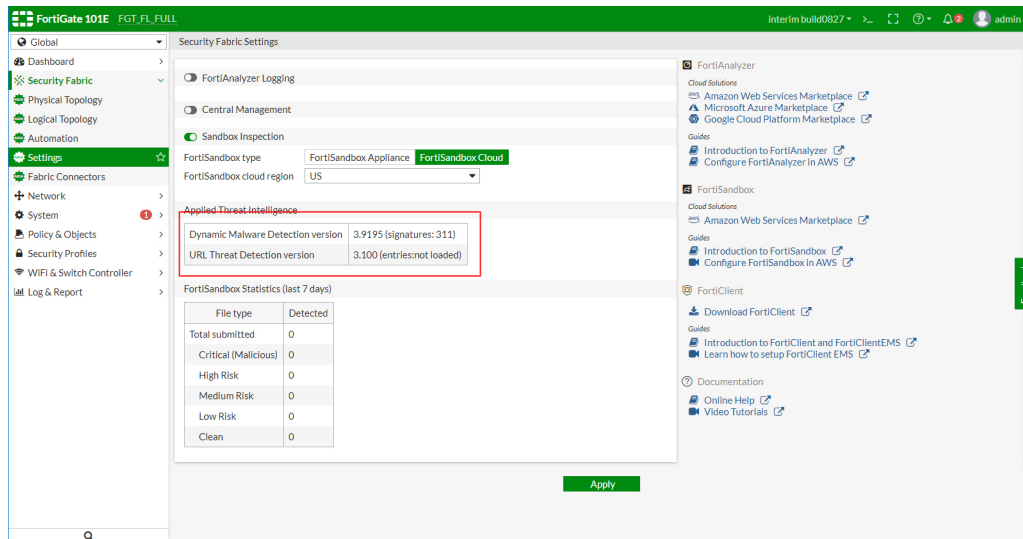
4. Select *FortiSandbox Cloud* and choose a region from the dropdown list.



5. Click *Apply* to save the settings.

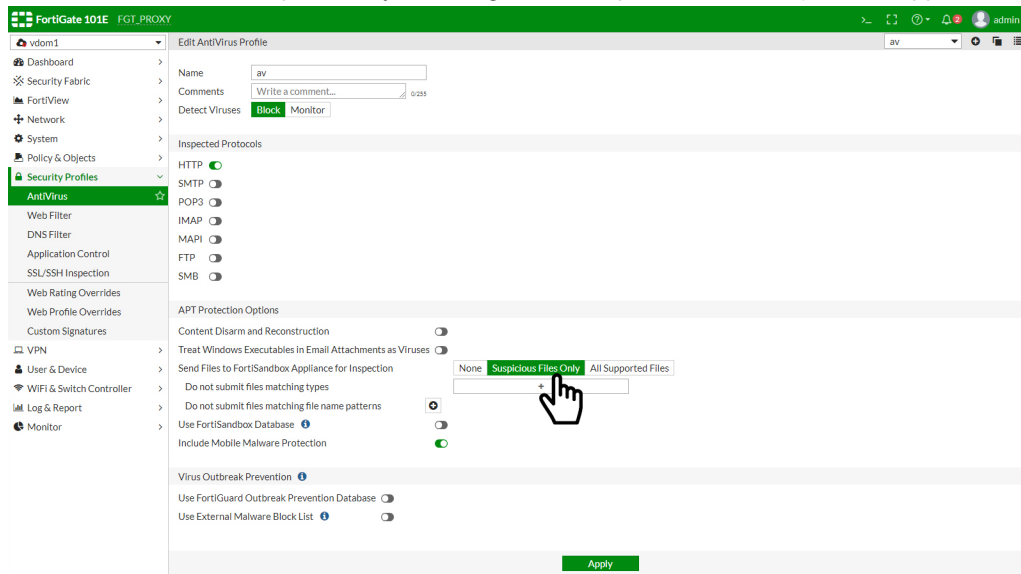


6. When the FortiGate is connected to the FortiSandbox Cloud, FortiSandbox's current database version is displayed.

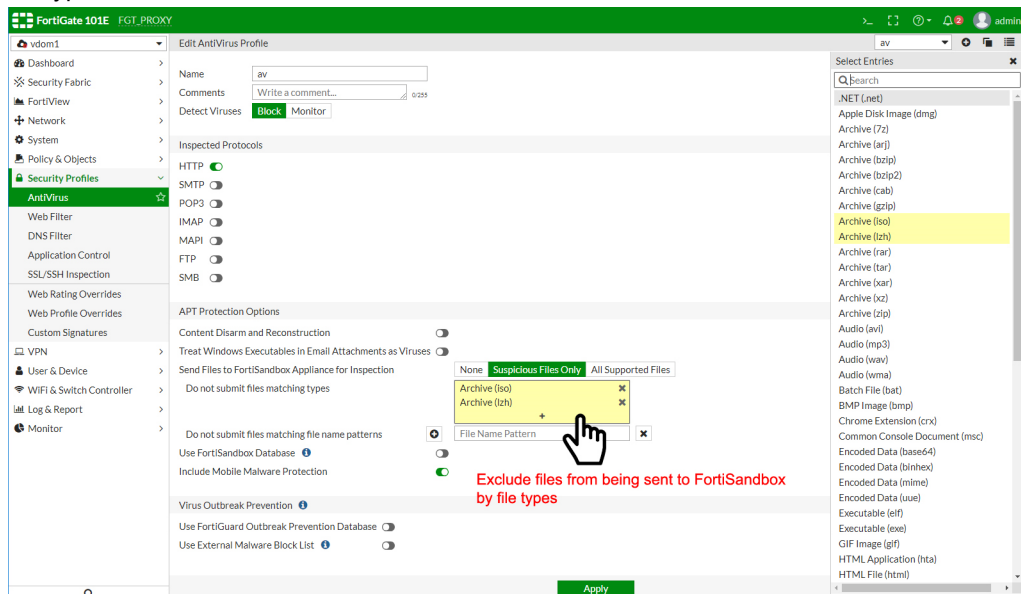


## To enable FortiSandbox inspection:

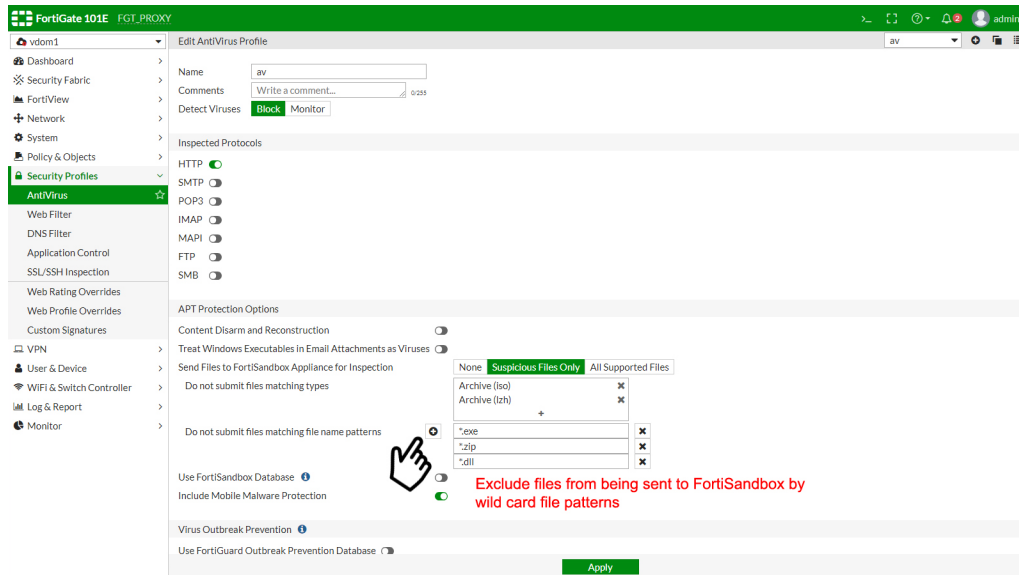
1. Go to *Security Profiles > AntiVirus*.
2. Enable FortiSandbox inspection by selecting either *Suspicious Files Only* or *All Supported Files*.



3. Files can be excluded from being sent to FortiSandbox based on their file types by choosing from a list of supported file types.



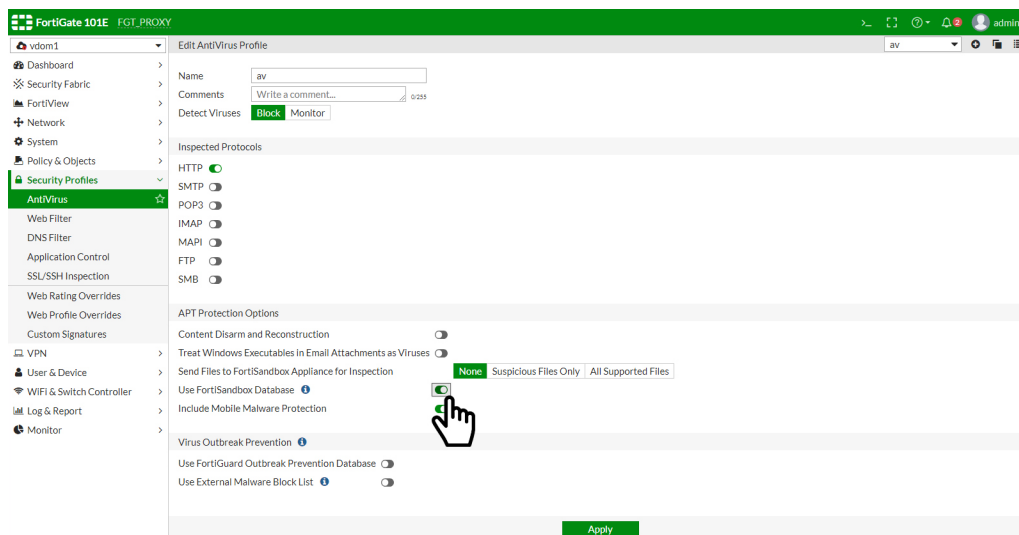
4. Files can also be excluded from being sent to FortiSandbox by using wildcard patterns.



5. Click *Apply*.

To enable the use of the FortiSandbox database:

1. Go to *Security Profiles > AntiVirus*.
2. Enable *Use FortiSandbox Database*.



3. Click *Apply*.

## Diagnostics and debugging

- Checking FortiGate Cloud controller status:

```
FGT_FL_FULL (global) # diagnose test application forticldd 2
Server: log-controller, task=0/10, watchdog is off
Domain name: logctrl11.fortinet.com
```

```
Address of log-controller: 1
 172.16.95.168:443
 Statistics: total=3, discarded=1, sent=2, last_updated=12163 secs ago
http connection: is not in progress
 Current address: 172.16.95.168:443
 Calls: connect=9, rxtx=12
Current tasks number: 0
Account: name=empty, status=0, type=basic
Current volume: 0B
Current tasks number: 0
Update timer fires in 74240 secs
```

- **Checking Cloud APT server status:**

```
FGT_FL_FULL (global) # diagnose test application forticldd 3
Debug zone info:
 Domain:
 Home log server: 0.0.0.0:0
 Alt log server: 0.0.0.0:0
 Active Server IP: 0.0.0.0
 Active Server status: down
 Log quota: 0MB
 Log used: 0MB
 Daily volume: 0MB
 fams archive pause: 0
 APTContract : 1 <====
 APT server: 172.16.102.51:514 <====
 APT Altserver: 172.16.102.52:514 <====
 Active APTServer IP: 172.16.102.51 <====
 Active APTServer status: up <====
```

- **FortiSandbox Cloud diagnostics:**

```
FGT_FL_FULL (global) # diagnose test application quarantine 1
Total remote&local devices: 4, any task full? 0
System have disk, vdom is enabled, mgmt=3, ha=1
xfer-fas is enabled: ips-archive dlp-archive, realtime=yes, taskfull=no
 addr=0.0.0.0/514, source-ip=0.0.0.0, keep-alive=no.
 ssl_opt=1, hmac_alg=0
 License=0, content_archive=0, arch_pause=0.

global-fas is disabled.
forticloud-fsb is enabled: analytics, realtime=yes, taskfull=no
 addr=172.16.102.51/514, source-ip=0.0.0.0, keep-alive=no.
 ssl_opt=1, hmac_alg=0
fortisandbox-fsb1 is disabled.
fortisandbox-fsb2 is disabled.
fortisandbox-fsb3 is disabled.
fortisandbox-fsb4 is disabled.
fortisandbox-fsb5 is disabled.
fortisandbox-fsb6 is disabled.
global-faz is disabled.
global-faz2 is disabled.
global-faz3 is disabled.
```

- Checking FortiSandbox Cloud submission statistics:

```
FGT_FL_FULL (global) # diagnose test application quarantined 2
Quarantine daemon state:
QUAR mem: mem_used=0, mem_limit=97269, threshold=72951
dropped(0 by quard, 0 by callers)
pending-jobs=0, tot-mem=0, last_ipc_run=12353, check_new_req=1
alloc_job_failed=0, job_wrong_type=0, job_wrong_req_len=0, job_invalid_qfd=0
tgz_create_failed=0, tgz_attach_failed=0, qfd_mmap_failed=0, buf_attached=0
xfer-fas:
 ips: total=0, handled=0, accepted=0
 quar: total=0, handled=0, accepted=0
 archive: total=0, handled=0, accepted=0
 analytics: total=0, handled=0, accepted=0, local_dups=0
 analytics stats: total=0, handled=0, accepted=0
 last_rx=0, last_tx=0, error_rx=0, error_tx=0
 max_num_tasks=10000, num_tasks=0, mem_used=0, ttl_drops=0, xfer_status=0
forticloud-fsb:
 ips: total=0, handled=0, accepted=0
 quar: total=0, handled=0, accepted=0
 archive: total=0, handled=0, accepted=0
 analytics: total=0, handled=0, accepted=0, local_dups=0
num_buffer=0(per-minute:10) last_min_count=0 last_vol_count=0 next_vol_reset_tm='Sun Feb
17 00:00:00 2019
'
 analytics stats: total=24, handled=24, accepted=24
 last_rx=1224329, last_tx=1224329, error_rx=2, error_tx=0
 max_num_tasks=200, num_tasks=0, mem_used=0, ttl_drops=0, xfer_status=0
```

- Checking FortiSandbox analysis statistics:

```
FGT_FL_FULL (global) # diagnose test application quarantine 7
Total: 0

Statistics:
 vfid: 0, detected: 0, clean: 0, risk_low: 0, risk_med: 0, risk_high: 0, limit_
reached:0
 vfid: 3, detected: 0, clean: 0, risk_low: 0, risk_med: 0, risk_high: 0, limit_
reached:0
 vfid: 4, detected: 0, clean: 0, risk_low: 0, risk_med: 0, risk_high: 0, limit_
reached:0

FGT_FL_FULL (global) #
```

- Update Daemon debug:

```
FGT_FL_FULL (global) # diagnose debug application quarantined -1
FGT_FL_FULL (global) # diagnose debug enable

quar_req_fsa_file()-890: fsa ext list new_version (1547781904)
quar_fsb_handle_quar()-1439: added a req-6 to fortisandbox-fsb5, vfid=1, oftp-name=[].
__quar_start_connection()-908: start server fortisandbox-fsb5-172.18.52.154 in vdom-1
[103] __ssl_cert_ctx_load: Added cert /etc/cert/factory/root_Fortinet_Factory.cer, root
ca Fortinet_CA, idx 0 (default)
[551] ssl_ctx_create_new_ex: SSL CTX is created
[578] ssl_new: SSL object is created
upd_cfg_extract_av_db_version[378]-version=06002000AVDB00201-00066.01026-1901301530
upd_cfg_extract_ids_db_version[437]-version=06002000NIDS02403-00014.00537-1901300043
```

```
upd_cfg_extract_ids_db_version[437]-version=06002000APDB00103-00006.00741-1512010230
upd_cfg_extract_ids_db_version[437]-version=06002000ISDB00103-00014.00537-1901300043
upd_cfg_extract_ibdb_botnet_db_version[523]-version=06002000IBDB00101-00004.00401-
1901281000
upd_cfg_extract_av_db_version[378]-version=06002000AVDB00201-00066.01026-1901301530
upd_cfg_extract_ids_db_version[437]-version=06002000NIDS02403-00014.00537-1901300043
upd_cfg_extract_ids_db_version[437]-version=06002000APDB00103-00006.00741-1512010230
upd_cfg_extract_ids_db_version[437]-version=06002000ISDB00103-00014.00537-1901300043
upd_cfg_extract_ibdb_botnet_db_version[523]-version=06002000IBDB00101-00004.00401-
1901281000
upd_cfg_extract_av_db_version[378]-version=06002000AVDB00201-00066.01026-1901301530
upd_cfg_extract_ids_db_version[437]-version=06002000NIDS02403-00014.00537-1901300043
upd_cfg_extract_ids_db_version[437]-version=06002000APDB00103-00006.00741-1512010230
upd_cfg_extract_ids_db_version[437]-version=06002000ISDB00103-00014.00537-1901300043
upd_cfg_extract_ibdb_botnet_db_version[523]-version=06002000IBDB00101-00004.00401-
1901281000
upd_cfg_extract_av_db_version[378]-version=06002000AVDB00201-00066.01026-1901301530
upd_cfg_extract_ids_db_version[437]-version=06002000NIDS02403-00014.00537-1901300043
upd_cfg_extract_ids_db_version[437]-version=06002000APDB00103-00006.00741-1512010230
upd_cfg_extract_ids_db_version[437]-version=06002000ISDB00103-00014.00537-1901300043
upd_cfg_extract_ibdb_botnet_db_version[523]-version=06002000IBDB00101-00004.00401-
1901281000
quar_remote_rcv_send()-731: dev=fortisandbox-fsb2 xfer-status=0
__quar_build_pkt()-408: build req(id=337, type=4) for vdom-vdom1, len=99, oftp_name=
__quar_send()-470: dev buffer -- pos=0, len=99
quar_remote_send()-520: req(id=337, type=4) read response, dev=fortisandbox-fsb2, xfer_
status=1, buflen=12
quar_remote_rcv_send()-770: dev=fortisandbox-fsb2, oevent=4, nevent=1, xfer-status=1
quar_remote_rcv_send()-731: dev=fortisandbox-fsb3 xfer-status=0
__quar_build_pkt()-408: build req(id=338, type=6) for vdom-vdom1, len=93, oftp_name=
__quar_send()-470: dev buffer -- pos=0, len=93
quar_remote_send()-520: req(id=338, type=6) read response, dev=fortisandbox-fsb3, xfer_
status=1, buflen=12
quar_remote_rcv_send()-770: dev=fortisandbox-fsb3, oevent=4, nevent=1, xfer-status=1
quar_remote_rcv_send()-731: dev=fortisandbox-fsb5 xfer-status=0
__quar_build_pkt()-408: build req(id=340, type=6) for vdom-vdom1, len=93, oftp_name=
__quar_send()-470: dev buffer -- pos=0, len=93
quar_remote_send()-520: req(id=340, type=6) read response, dev=fortisandbox-fsb5, xfer_
status=1, buflen=12
quar_remote_rcv_send()-770: dev=fortisandbox-fsb5, oevent=4, nevent=1, xfer-status=1
quar_remote_rcv_send()-731: dev=fortisandbox-fsb2 xfer-status=1
quar_remote_rcv()-662: dev(fortisandbox-fsb2) received a packet: len=69, type=1
quar_remote_rcv()-718: file-[337] is accepted by server(fortisandbox-fsb2).
quar_put_job_req()-332: Job 337 deleted
quar_remote_rcv_send()-731: dev=fortisandbox-fsb4 xfer-status=0
__quar_build_pkt()-408: build req(id=339, type=6) for vdom-vdom1, len=93, oftp_name=
__quar_send()-470: dev buffer -- pos=0, len=93
quar_remote_send()-520: req(id=339, type=6) read response, dev=fortisandbox-fsb4, xfer_
status=1, buflen=12
quar_remote_rcv_send()-770: dev=fortisandbox-fsb4, oevent=4, nevent=1, xfer-status=1
```

```

quar_remote_rcv_send()-731: dev=fortisandbox-fsbl xfer-status=0
__quar_build_pkt()-408: build req(id=336, type=4) for vdom-root, len=98, oftp_name=
__quar_send()-470: dev buffer -- pos=0, len=98
...
__get_analytics_stats()-19: Received an ANALYTICS_STATS request, vfid: 0
__quar_req_handler()-127: Request 0 was handled successfully
__get_analytics_stats()-19: Received an ANALYTICS_STATS request, vfid: 0
__quar_req_handler()-127: Request 0 was handled successfully
__get_analytics_stats()-19: Received an ANALYTICS_STATS request, vfid: 0
__quar_req_handler()-127: Request 0 was handled successfully
__get_analytics_stats()-19: Received an ANALYTICS_STATS request, vfid: 0
__quar_req_handler()-127: Request 0 was handled successfully
quar_fsb_handle_quar()-1439: added a req-6 to fortisandbox-fsbl, vfid=1, oftp-name=[].
__quar_start_connection()-908: start server fortisandbox-fsbl-172.18.52.154 in vdom-1
[103] __ssl_cert_ctx_load: Added cert /etc/cert/factory/root_Fortinet_Factory.cer, root
ca Fortinet_CA, idx 0 (default)
[551] ssl_ctx_create_new_ex: SSL CTX is created
[578] ssl_new: SSL object is created
upd_cfg_extract_av_db_version[378]-version=06002000AVDB00201-00066.01026-1901301530
upd_cfg_extract_ids_db_version[437]-version=06002000NIDS02403-00014.00537-1901300043
upd_cfg_extract_ids_db_version[437]-version=06002000APDB00103-00006.00741-1512010230
upd_cfg_extract_ids_db_version[437]-version=06002000ISDB00103-00014.00537-1901300043
upd_cfg_extract_ibdb_botnet_db_version[523]-version=06002000IBDB00101-00004.00401-
1901281000
quar_remote_rcv_send()-731: dev=fortisandbox-fsbl xfer-status=0
__quar_build_pkt()-408: build req(id=2, type=6) for vdom-vdom1, len=93, oftp_name=
__quar_send()-470: dev buffer -- pos=0, len=93
quar_remote_send()-520: req(id=2, type=6) read response, dev=fortisandbox-fsbl, xfer_
status=1, buflen=12
quar_remote_rcv_send()-770: dev=fortisandbox-fsbl, oevent=4, nevent=1, xfer-status=1
quar_remote_rcv_send()-731: dev=fortisandbox-fsbl xfer-status=1
quar_remote_rcv()-662: dev(fortisandbox-fsbl) received a packet: len=767, type=1
quar_store_analytics_report()-590: Analytics-report return
file=/tmp/fsb/83bb2d9928b03a68b123730399b6b9365b5cc9a5a77f8aa007a6f1a499a13b18.json.gz,
buf_sz=735
quar_store_analytics_report()-597: The request
'83bb2d9928b03a68b123730399b6b9365b5cc9a5a77f8aa007a6f1a499a13b18' score is 1
quar_remote_rcv()-718: file-[2] is accepted by server(fortisandbox-fsbl).
quar_put_job_req()-332: Job 2 deleted
quar_monitor_connection_func()-978: monitoring dev fortisandbox-fsbl
quar_monitor_connection_func()-978: monitoring dev fortisandbox-fsbl
__get_analytics_stats()-19: Received an ANALYTICS_STATS request, vfid: 0
__quar_req_handler()-127: Request 0 was handled successfully
__get_analytics_stats()-19: Received an ANALYTICS_STATS request, vfid: 0
__quar_req_handler()-127: Request 0 was handled successfully
quar_monitor_connection_func()-978: monitoring dev fortisandbox-fsbl
quar_stop_connection()-1006: close connection to server(fortisandbox-fsbl)
[193] __ssl_data_ctx_free: Done
[805] ssl_free: Done
[185] __ssl_cert_ctx_free: Done
[815] ssl_ctx_free: Done
[796] ssl_disconnect: Shutdown

```

- **Appliance FortiSandbox diagnostics:**

```

FGT_PROXY # config global
FGT_PROXY (global) # diagnose test application quarantined 1

```



```
Total remote&local devices: 8, any task full? 0
System have disk, vdom is enabled, mgmt=1, ha=2
xfer-fas is enabled: ips-archive dlp-archive, realtime=yes, taskfull=no
 addr=0.0.0.0/514, source-ip=0.0.0.0, keep-alive=no.
 ssl_opt=0, hmac_alg=0
 License=0, content_archive=0, arch_pause=0.

global-fas is disabled.
forticloud-fsb is disabled.
fortisandbox-fsb1 is enabled: analytics, realtime=yes, taskfull=no
 addr=172.18.52.154/514, source-ip=0.0.0.0, keep-alive=no.
 ssl_opt=3, hmac_alg=0
fortisandbox-fsb2 is enabled: analytics, realtime=yes, taskfull=no
 addr=172.18.52.154/514, source-ip=0.0.0.0, keep-alive=no.
 ssl_opt=3, hmac_alg=0
fortisandbox-fsb3 is enabled: analytics, realtime=yes, taskfull=no
 addr=172.18.52.154/514, source-ip=0.0.0.0, keep-alive=no.
 ssl_opt=3, hmac_alg=0
fortisandbox-fsb4 is enabled: analytics, realtime=yes, taskfull=no
 addr=172.18.52.154/514, source-ip=0.0.0.0, keep-alive=no.
 ssl_opt=3, hmac_alg=0
fortisandbox-fsb5 is enabled: analytics, realtime=yes, taskfull=no
 addr=172.18.52.154/514, source-ip=0.0.0.0, keep-alive=no.
 ssl_opt=3, hmac_alg=0
fortisandbox-fsb6 is enabled: analytics, realtime=yes, taskfull=no
 addr=172.18.52.154/514, source-ip=0.0.0.0, keep-alive=no.
 ssl_opt=3, hmac_alg=0
global-faz is disabled.
global-faz2 is disabled.
global-faz3 is disabled.
```

## Web filter

Web filtering restricts or controls user access to web resources and can be applied to firewall policies.

In FortiOS, there are three main components of web filtering:

- Web content filter: blocks web pages containing words or patterns that you specify.
- URL filter: uses URLs and URL patterns to block or exempt web pages from specific sources, or block malicious URLs discovered by FortiSandbox.
- FortiGuard Web Filtering service: provides many additional categories you can use to filter web traffic.

These components interact with each other to provide maximum control over what users on your network can view and protect your network from many internet content threats.

Web filters are applied in the following order:

1. URL filter
2. FortiGuard Web Filtering
3. Web content filter
4. Web script filter
5. Antivirus scanning

FortiOS includes three preloaded web filter profiles:

- *default*
- *monitor-all* (monitors and logs all URLs visited, flow-based)
- *wifi-default* (default configuration for offloading WiFi traffic)

You can customize these profiles, or you can create your own to manage network user access.



Some features of this functionality require a subscription to FortiGuard Web Filtering.

---

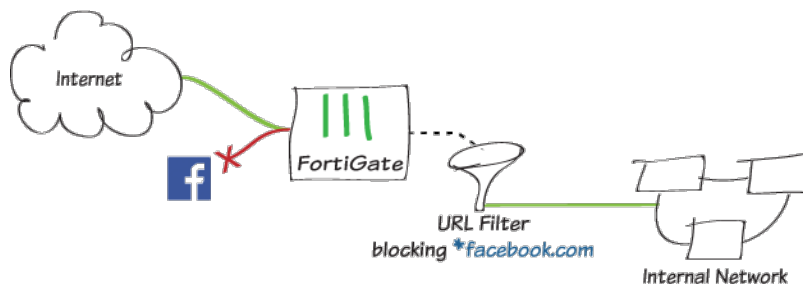
The following topics provide information about web filters:

- [URL filter on page 948](#)
- [FortiGuard filter on page 954](#)
- [Usage quota on page 961](#)
- [Web content filter on page 963](#)
- [File filter on page 967](#)
- [Advanced filters 1 on page 973](#)
- [Advanced filters 2 on page 977](#)
- [External resources for web filter on page 982](#)
- [Reliable web filter statistics on page 988](#)
- [Flow-based web filtering on page 991](#)
- [URL certificate blocklist on page 993](#)

## URL filter

URL filter is also called static URL filter. By adding specific URLs with patterns containing text and regular expressions, FortiGate can allow, block, exempt, and monitor web pages matching any specified URLs or patterns, and can display a replacement message instead.

### Sample topology



### Create URL filter

You can create a URL filter using the GUI or CLI. After creating the URL filter, attach it to a web filter profile.

**To create URL filter in the GUI:**

1. Go to *Security Profiles > Web Filter* and go to the *Static URL Filter* section.
2. Enable *URL Filter*.

Static URL Filter

Block invalid URLs ☐

URL Filter ☒

+ Create New Edit Delete Search

URL	Type	Action	Status	Referrer
No results				

Block malicious URLs discovered by FortiSandbox ☐

Content Filter ☐

3. Under *URL Filter*, click *Create New* to display the *New URL Filter* pane.

New URL Filter

URL

Type **Simple** Regular Expression Wildcard

Action **Exempt** Block Allow Monitor

Status **Enable** Disable

Referrer

OK Cancel

URL Filter Type	Description
<b>Simple</b>	FortiGate tries to strictly match the full context. For example, if you enter <i>www.facebook.com</i> in the <i>URL</i> field, it only matches traffic with <i>www.facebook.com</i> . It won't match <i>facebook.com</i> or <i>message.facebook.com</i> . When FortiGate finds a match, it performs the selected <i>URL Action</i> .
<b>Regular Expression or Wildcard</b>	FortiGate tries to match the pattern based on the rules of regular expressions or wildcards. For example, if you enter <i>*fa*</i> in the <i>URL</i> field, it matches all the content that has <i>fa</i> such as <i>www.facebook.com</i> , <i>message.facebook.com</i> , <i>fast.com</i> , etc. When FortiGate finds a match, it performs the selected <i>URL Action</i> .

For more information, see the URL Filter expressions technical note in <https://kb.fortinet.com/kb/documentLink.do?externalID=FD37057>.

URL Filter Action	Description
<b>Block</b>	Denies or blocks attempts to access any URL matching the URL pattern. FortiGate displays a replacement message.
<b>Allow</b>	The traffic is passed to the remaining FortiGuard web filters, web content filters, web script filters, antivirus proxy operations, and DLP proxy operations. If the URL does not appear in the URL list, the traffic is permitted.
<b>Monitor</b>	The traffic is processed the same way as the <i>Allow</i> action. For the <i>Monitor</i> action, a log message is generated each time a matching traffic pattern is established.
<b>Exempt</b>	The traffic is allowed to bypass the remaining FortiGuard web filters, web content filters, web script filters, antivirus scanning, and DLP proxy operations

4. Enter *\*facebook.com*, select *Wildcard*, and select *Block*.

Static URL Filter

Block invalid URLs ☐

URL Filter ☒

URL	Type	Action	Status
*facebook.com	Wildcard	Block	Enable

Block malicious URLs discovered by FortiSandbox ☐

Content Filter ☐

5. Click *OK*.

After creating the URL filter, attach it to a webfilter profile.

### Create URL filter using CLI

To create and enable a URL filter using the CLI, create the URL filter and then attach it to a `webfilter` profile. The CLI commands below show the full configuration of creating a URL filter.

```
config webfilter urlfilter
edit {id}
Configure URL filter lists.
set name {string} Name of URL filter list. size[35]
config entries
edit {id}
URL filter entries.
set url {string} URL to be filtered. size[511]
set type {simple | regex | wildcard} Filter type (simple, regex, or wildcard).
 simple Simple URL string.
 regex Regular expression URL string.
 wildcard Wildcard URL string.
set action {exempt | block | allow | monitor} Action to take for URL filter
matches.
 exempt Exempt matches.
 block Block matches.
 allow Allow matches (no log).
 monitor Allow matches (with log).
set status {enable | disable} Enable/disable this URL filter.
set exempt {option} If action is set to exempt, select the security profile
operations that exempt URLs skip. Separate multiple options with a space.
 av AntiVirus scanning.
 web-content Web Filter content matching.
 activex-java-cookie ActiveX, Java, and cookie filtering.
 dlp DLP scanning.
 fortiguard FortiGuard web filter.
 range-block Range block feature.
 pass Pass single connection from all.
 all Exempt from all security profiles.
set referrer-host {string} Referrer host name. size[255]
next
end
```

**To create URL filter to filter Facebook using the CLI:**

```

config webfilter urlfilter
 edit 1
 set name "webfilter"
 config entries
 edit 1
 set url "*facebook.com"
 set type wildcard
 set action block
 next
 end
 next
end

```

**To attach the URL filter to a web filter profile:**

```

config webfilter profile
 edit "webfilter" <-- the name of the webfilter profile
 config web
 set urlfilter-table 1 <-- the URL filter created with ID number 1
 end
 config ftgd-wf
 unset options
 end
 next
end

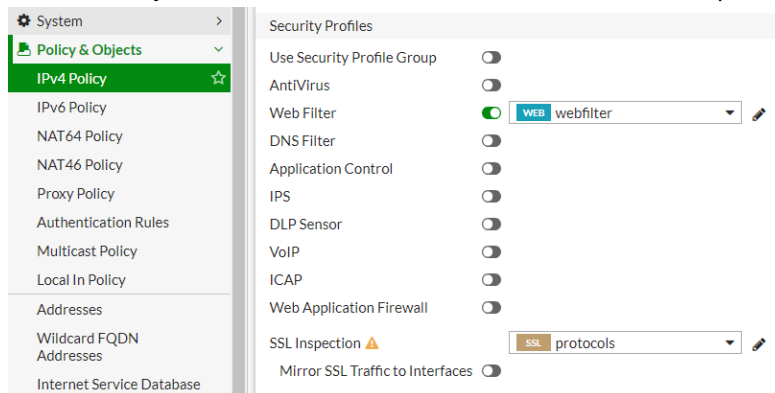
```

**Attach web filter profile to the firewall policy**

After you have created the URL filter and attached it to a web filter profile, you must attach the profile to a firewall policy.

**To attach a web filter profile to a firewall policy using the GUI:**

1. Go to *Policy & Objects > IPv4 Policy*.
2. Edit the policy that you want to enable the web filter.
3. In the *Security Profiles* section, enable *Web Filter* and select the profile you created.



4. Click **OK**.

**To attach a web filter profile to a firewall policy using the CLI:**

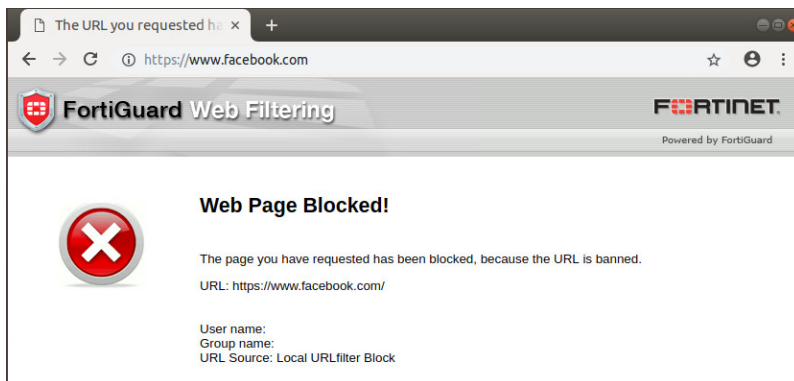
```

config firewall policy
 edit 1
 set name "WF"
 set uuid b725a4d4-5be5-51e9-43fa-6d4e67d56bad
 set srcintf "wan2"
 set dstintf "wan1"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set utm-status enable
 set inspection-mode proxy
 set logtraffic all
 set webfilter-profile "webfilter" <-- attach the webfilter profile you just
created.
 set profile-protocol-options "protocol"
 set ssl-ssh-profile "protocols"
 set nat enable
 next
end

```

**Validate the URL filter results**

Validate the URL filter results by going to a blocked website. For example, when you go to the Facebook website, you see the replacement message.

**To customize the URL web page blocked message:**

1. Go to *System > Replacement Messages*.
2. Go to the *Security* section and select *URL Block Page*.

### 3. Set up a custom message for blocked pages.

The screenshot shows the FortiGate GUI's Security Profiles configuration page. The left sidebar shows the navigation menu with 'Security Profiles' selected. The main area displays a table of replacement HTML messages for various security events. The 'URL Block Page' is highlighted in yellow. Below the table, a preview of the blocked page is shown, featuring a red 'X' icon and the text 'Web Page Blocked!'. The preview also displays the URL being blocked and the user information.

Category	Event	Replacement HTML
Authentication (4)	Device Detection Portal Failure Page	Replacement HTML for device detection portal failure page
	Email Collection	Replacement HTML for email collection page
	Email Collection Invalid Email	Replacement HTML for email collection page after user enters invalid email
	FortiToken Page	Replacement HTML for FortiToken authentication page
Login Page	Login Failed Page	Replacement HTML for authentication failed page
	Login Page	Replacement HTML for authentication login page
Security (7)	Application Control Block Page	Replacement HTML for application control block page
	DLP Block Message	Replacement text for DLP block message
	DLP Block Page	Replacement HTML for DLP block page
	FortiGuard Block Page	Replacement HTML for FortiGuard Web Filter block page
	URL Block Page	Replacement HTML for HTTP URL blocked page
Virus Block Message	Virus Block Message	Replacement text for antivirus block message
	Virus Block Page	Replacement HTML for antivirus block page
SSL VPN (2)	SSL VPN Login Page	Replacement HTML for SSL VPN login page
	SSL VPN Portal Header	Replacement HTML for SSL VPN portal page header

Message Format: text/html Message Size: 2.9 KB/32.8 KB

**Web Page Blocked!**

The page you have requested has been blocked, because the URL is banned.

URL: http://www.example.com/

Request Blocked  
User name: Guest  
Group name: Guest-group  
URL Source: Blocking Source

override

### To check web filter logs in the GUI:

#### 1. Go to Log & Report > Web Filter.

The screenshot shows the FortiGate GUI's Log & Report page. The left sidebar shows the navigation menu with 'Log & Report' selected. The main area displays a table of log entries. The 'Web Filter' log is selected, and a log entry is highlighted. The log details are shown on the right.

Date/Time	User	Source	Action	URL
2019/04/22 11:48:43		10.1.200.15	blocked	www.facebook.com/favicon.ico
2019/04/22 11:48:43		10.1.200.15	blocked	www.facebook.com/
2019/04/22 11:48:41		10.1.200.15	passthrough	www.google.com/complete/search?client=chrome-omni&gs_l=chrome-ext-ansg&ssli=t&q=&olt=

**Log Details**

**General**

Date: 2019/04/22  
Time: 11:48:43  
Session ID: 649063  
Virtual Domain: vdom1

**Source**

IP: 10.1.200.15  
Source Port: 50472  
Source Interface: wan2  
User:

**Destination**

IP: 157.240.18.35  
Port: 443  
Destination: wan1  
Interface: wan1  
Hostname: www.facebook.com  
URL: www.facebook.com/

**Application Control**

Protocol: 6  
Service: HTTPS

**Data**

Received Bytes: 141 B  
Sent Bytes: 1 kB

**Action**

#### 2. If there are too many log entries, click **Add Filter** and select **Event Type > URL Filter** to display logs generated by the URL filter.

### To check web filter logs in the CLI:

```
execute log filter category utm-webfilter
```

```
execute log display
```

```
1: date=2019-04-22 time=11:48:43 logid="0315012544" type="utm" subtype="webfilter"
eventtype="urlfilter" level="warning" vd="vdom1" eventtime=1555958923322174610
urlfilteridx=0 urlsource="Local URLfilter Block" policyid=1 sessionid=649063
srcip=10.1.200.15 srcport=50472 srcintf="wan2" srcintfrole="wan" dstip=157.240.18.35
dstport=443 dstintf="wan1" dstintfrole="wan" proto=6 service="HTTPS"
hostname="www.facebook.com" profile="webfilter" action="blocked" reqtype="direct" url="/"
sentbyte=1171 rcvbyte=141 direction="outgoing" msg="URL was blocked because it is in the
URL filter list" crscore=30 craction=8 crlevel="high"
```

## FortiGuard filter

To use this service, you must have a valid subscription on your FortiGate.

FortiGuard filter enhances the web filter features supplied with your FortiGate unit by sorting billions of web pages into a wide range of categories that users can allow or block.

The FortiGuard Web Filtering service includes over 45 million individual website ratings that apply to more than two billion pages. When the FortiGuard filter is enabled in a web filter and is applied to firewall policies, if a request for a web page appears in traffic controlled by one of the firewall policies, the URL is sent to the nearest FortiGuard server. The URL category or rating is returned. If the category is blocked, the FortiGate shows a replacement message in place of the requested page. If the category is not blocked, the page request is sent to the requested URL as normal.

### FortiGuard web filter actions

You can select one of the following FortiGuard web filter actions:

FortiGuard Web Filter Action	Description
<b>Allow</b>	Permit access to the sites in the category.
<b>Block</b>	Prevent access to the sites in the category. Users trying to access a blocked site sees a replacement message indicating the site is blocked.
<b>Monitor</b>	Permits and logs access to sites in the category. You can enable user quotas when you enable this action.
<b>Warning</b>	Displays a message to the user allowing them to continue if they choose.
<b>Authenticate</b>	Requires the user to authenticate with the FortiGate before allowing access to the category or category group.

### FortiGuard web filter categories

FortiGuard has many web filter categories including two local categories and a special remote category. For more information on the different categories, see the table below.

FortiGuard Web Filter category	Where to find more information
All URL categories	<a href="https://fortiguard.com/webfilter/categories">https://fortiguard.com/webfilter/categories</a>
Local categories	<a href="#">Web rating override on page 1102</a>
Remote category	<a href="#">External resources for web filter on page 982</a>

The priority of categories is local category > external category > FortiGuard built-in category. If a URL is configured as a local category, it only follows the behavior of local category and not external or FortiGuard built-in category.

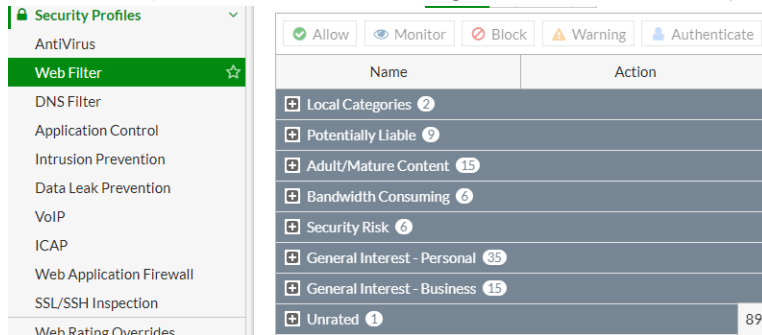
### Sample configuration of blocking a web category

This example shows blocking a website based on its category (rating), for example, information technology.

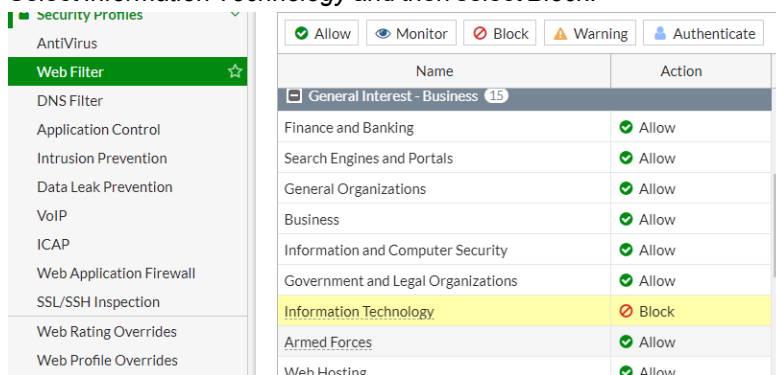


## To block a category in the GUI:

1. Go to *Security Profiles > Web Filter* and go to the *FortiGuard category based filter* section.



2. Open the *General Interest - Business* section by clicking the + icon beside it.
3. Select *Information Technology* and then select *Block*.

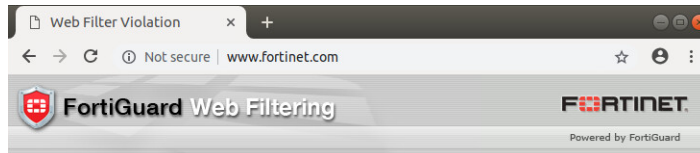


## To block a category in the CLI:

```
config webfilter profile
 edit "webfilter"
 config ftgd-wf
 unset options
 config filters
 edit 1
 set category 52 -- the pre-set id of "information technology"
 caterogy
 set action block -- set action to block
 next
 end
 end
 next
end
```

## To validate that you have blocked a category:

1. Go to a website belonging to the blocked category, for example, [www.fortinet.com](http://www.fortinet.com), and you see a blocked page and the category that is blocked.



### Web Page Blocked!

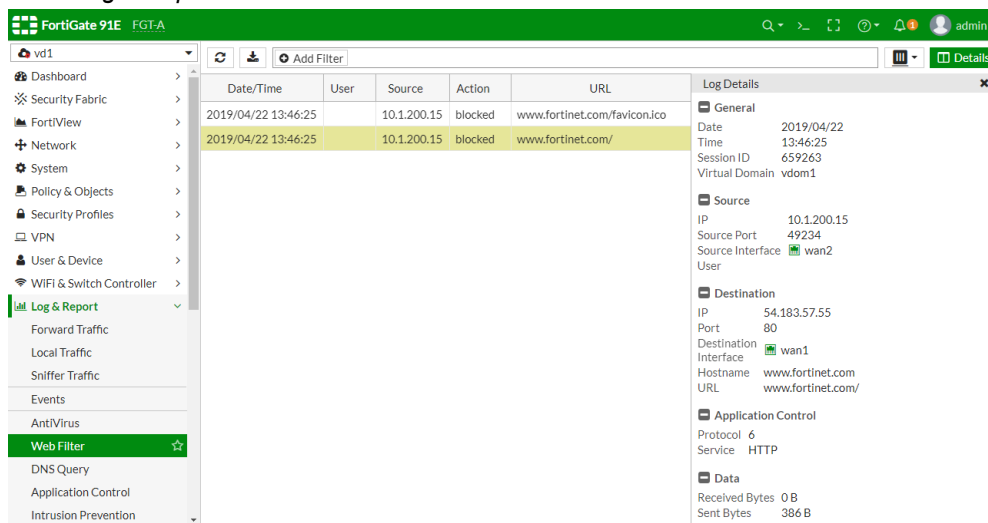
You have tried to access a web page which is in violation of your internet usage policy.

URL: <http://www.fortinet.com/>  
 Category: Information Technology  
 User name:  
 Group name:

To have the rating of this web page re-evaluated [please click here](#).

## To view the log of a blocked website in the GUI:

1. Go to **Log & Report > Web Filter**.



## To view the log of a blocked website in the CLI:

```
FGT52E-NAT-WF # execute log filter category utm-webfilter
```

```
FGT52E-NAT-WF # execute log display
```

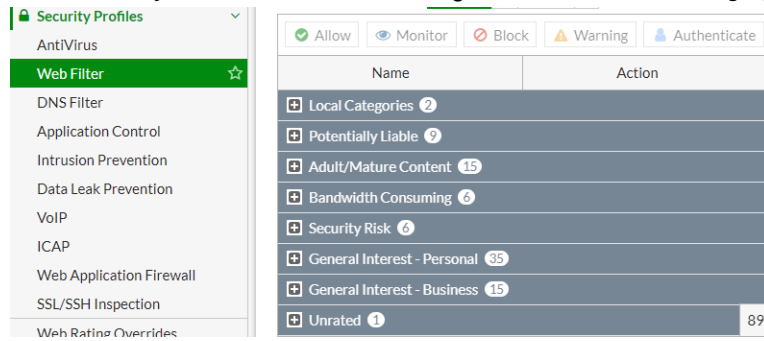
```
1: date=2019-04-22 time=13:46:25 logid="0316013056" type="utm" subtype="webfilter"
eventtype="ftgd_blk" level="warning" vd="vdom1" eventtime=1555965984972459609 policyid=1
sessionid=659263 srcip=10.1.200.15 srcport=49234 srcintf="wan2" srcintfrole="wan"
dstip=54.183.57.55 dstport=80 dstintf="wan1" dstintfrole="wan" proto=6 service="HTTP"
hostname="www.fortinet.com" profile="webfilter" action="blocked" reqtype="direct" url="/"
sentbyte=386 rcvdbyte=0 direction="outgoing" msg="URL belongs to a denied category in
policy" method="domain" cat=52 catdesc="Information Technology"
```

## Sample configuration of issuing a warning

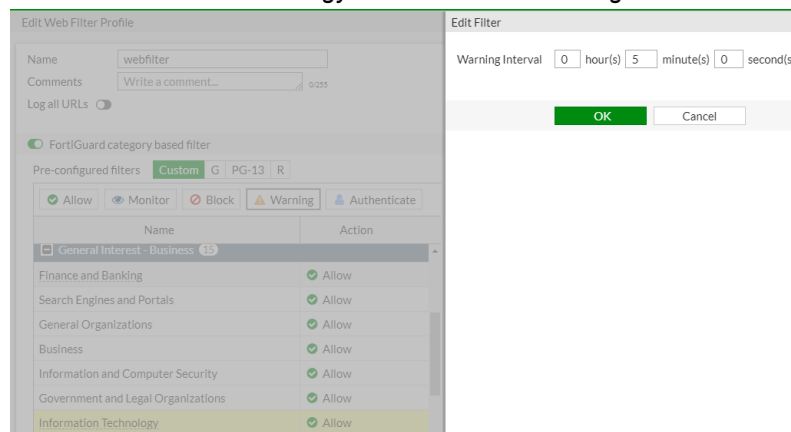
This example shows issuing a warning when a user visits a website based on its category (rating), for example, information technology.

### To configure a warning in the GUI:

1. Go to *Security Profiles > Web Filter* and go to the *FortiGuard category based filter* section.



2. Open the *General Interest - Business* section by clicking the + icon beside it.
3. Select *Information Technology* and then select *Warning*.



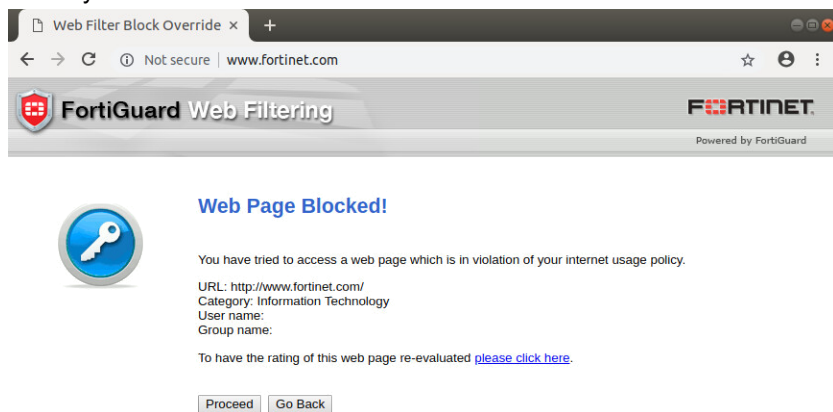
4. Set the *Warning Interval* which is the interval when the warning page appears again after the user chooses to continue.

### To configure a warning in the CLI:

```
config webfilter profile
 edit "webfilter"
 config ftgd-wf
 unset options
 config filters
 edit 1
 set category 52
 set action warning -- set action to warning
 next
 end
 end
 next
end
```

## To validate that you have configured the warning:

1. Go to a website belonging to the selected category, for example, [www.fortinet.com](http://www.fortinet.com), and you see a warning page where you can choose to *Proceed* or *Go Back*.

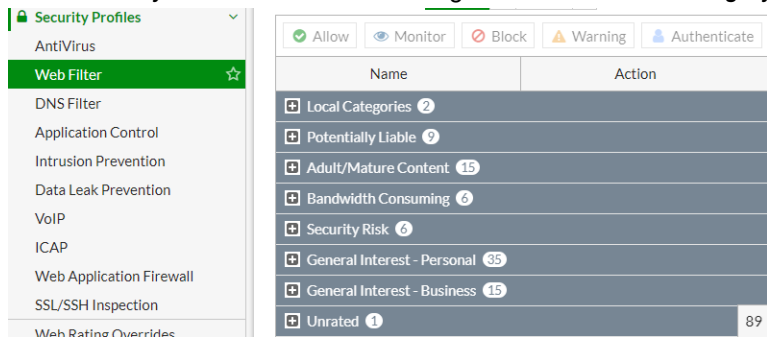


## Sample configuration of authenticating a web category

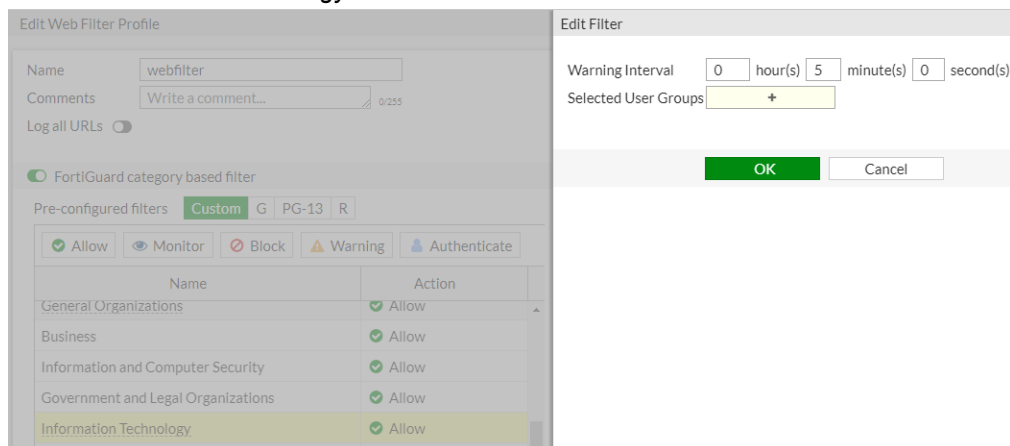
This example shows authenticating a website based on its category (rating), for example, information technology.

### To authenticate a category in the GUI:

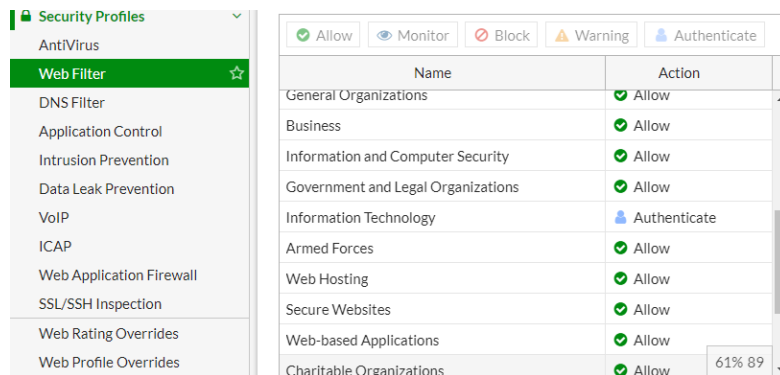
1. Go to *Security Profiles > Web Filter* and go to the *FortiGuard category based filter* section.



2. Open the *General Interest - Business* section by clicking the + icon beside it.
3. Select *Information Technology* and then select *Authenticate*.



4. Set the *Warning Interval* which is the interval when the authentication page appears again after authentication.
5. Click the + icon beside Selected User Group and select a user group. You must have a valid user group to use this feature.

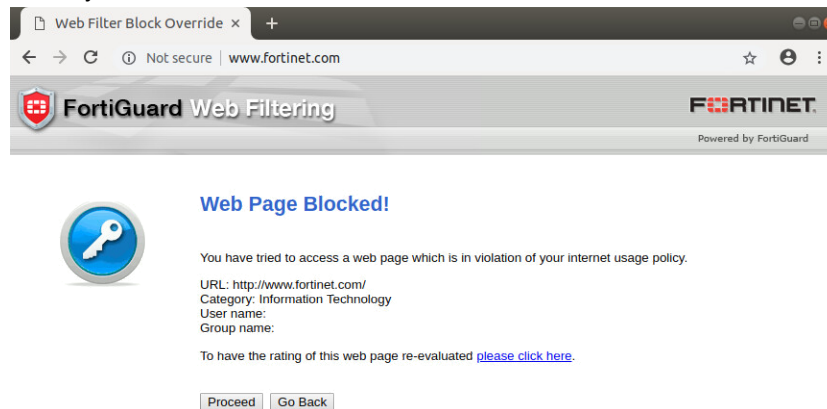


### To authenticate a category in the CLI:

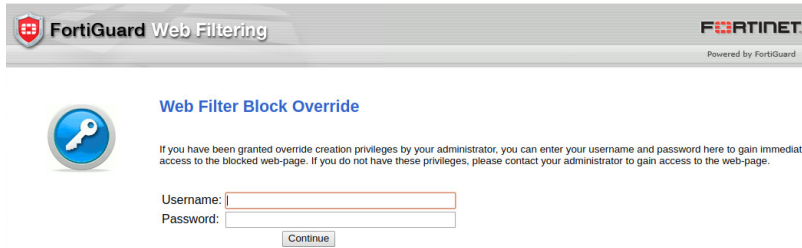
```
config webfilter profile
 edit "webfilter"
 config ftgd-wf
 unset options
 config filters
 edit 1
 set category 52
 set action authenticate -- set the action of authenticate
 set auth-usr-grp "local_group" -- user to authenticate
 next
 end
 end
 next
end
```

### To validate that you have configured authentication:

1. Go to a website belonging to the selected category, for example, [www.fortinet.com](http://www.fortinet.com). First, you see a warning page where you can choose to *Proceed* or *Go Back*.



- Click *Proceed* to check that the authentication page appears.



The screenshot shows the FortiGuard Web Filtering authentication page. At the top, there's a header with the FortiGuard logo and 'Powered by FortiGuard'. Below the header, there's a section titled 'Web Filter Block Override' with a key icon. A text box explains that users with override privileges can enter their username and password to gain immediate access to blocked web-pages. Below this, there are input fields for 'Username:' and 'Password:', followed by a 'Continue' button.

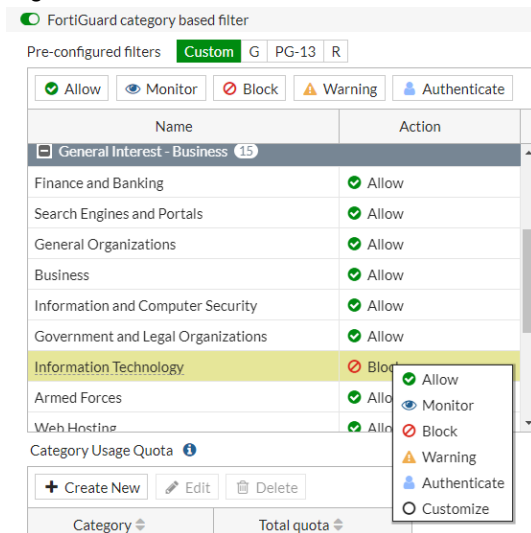
- Enter the username and password of the user group you selected, and click *Continue*.  
If the credentials are correct, the traffic is allowed through.

## Sample customization of the replacement page

When the FortiGuard Web Filter action is *Block*, *Warning*, or *Authenticate*, there is a *Customize* option for you to customize the replace page.

### To customize the replace page:

- Go to *Security Profiles > Web Filter* and go to the *FortiGuard category based filter* section.
- Right-click the item and select *Customize*.



The screenshot shows the 'FortiGuard category based filter' configuration page. At the top, there's a toggle for 'FortiGuard category based filter' and a 'Pre-configured filters' section with buttons for 'Custom', 'G', 'PG-13', and 'R'. Below this, there's a table with columns 'Name' and 'Action'. The table lists various categories and their corresponding actions. A context menu is open over the 'Information Technology' row, showing options: 'Allow', 'Monitor', 'Block', 'Warning', 'Authenticate', and 'Customize'. The 'Customize' option is selected.

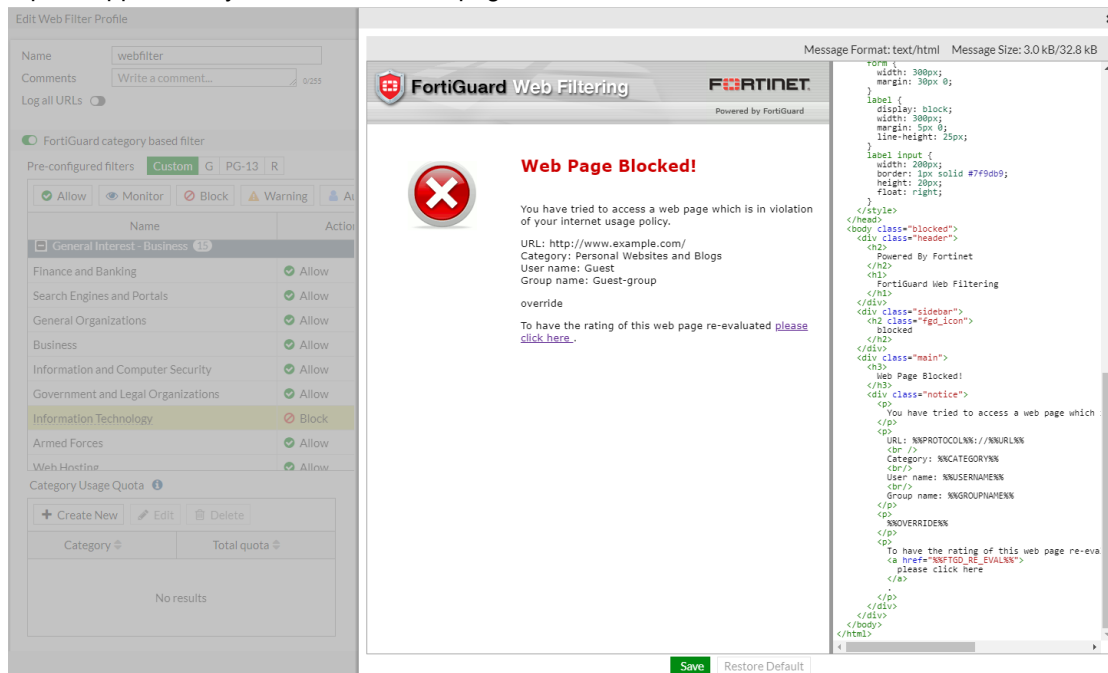
Name	Action
General Interest - Business	15
Finance and Banking	Allow
Search Engines and Portals	Allow
General Organizations	Allow
Business	Allow
Information and Computer Security	Allow
Government and Legal Organizations	Allow
Information Technology	Block
Armed Forces	Allow
Web Hosting	Allow

Category Usage Quota

+ Create New Edit Delete

Category Total quota

### 3. A pane appears for you to customize the page.



## Usage quota

In addition to using category and classification blocks and overrides to limit user access to URLs, you can set a daily quota by category, category group, or classification. Quotas allow access for a specified length of time or a specific bandwidth, and is calculated separately for each user. Quotas are reset everyday at midnight.

Quotas can be set only for the actions of *Monitor*, *Warning*, or *Authenticate*. When the quota is reached, the traffic is blocked and the replacement page displays.



You can only use quotas when inspection mode is *Proxy*.

## Sample topology



## Sample configuration of setting a quota

This example shows setting a time quota for a category, for example, the Education category.

### To configure a quota in the GUI:

1. Go to *Security Profiles > Web Filter* and go to the *FortiGuard category based filter* section.
2. Open the *General Interest - Personal* section by selecting the + icon beside it.
3. Select *Education* and then select *Monitor*.
4. In the *Category Usage Quota* section, select *Create New*.

FortiGuard category based filter

☒ Allow
 ☒ Monitor
 ☐ Block
 ☐ Warning
 ☐ Authenticate

Name	Action	Override Replacement Message	Selected User Groups	Warning Interval
General Interest - Personal	35			
Advertising	Allow			
Brokerage and Trading	Allow			
Games	Allow			
Web-based Email	Allow			
Entertainment	Allow			
Arts and Culture	Allow			
Education	Mon...			
Health and Wellness	Allow			

Category Usage Quota

Create New
  Edit
  Delete

Category	Total quota
No results	

5. In the right pane, select the *Category* field and then select *Education*.
6. For the *Quota Type*, select *Time* and set the *Total quota* to 5 minute(s).

New/Edit Quota

Category: Education

Quota Type: ☒ Time ☐ Traffic

Total quota: 0 hour(s) 5 minute(s) 0 second(s)

OK
  Cancel

7. Select *OK* and the *Category Usage Quota* section displays the quota.

Education: Mon...

Health and Wellness: Allow

Category Usage Quota

Create New
  Edit
  Delete

Category	Total quota
Education	5 minute(s)

1

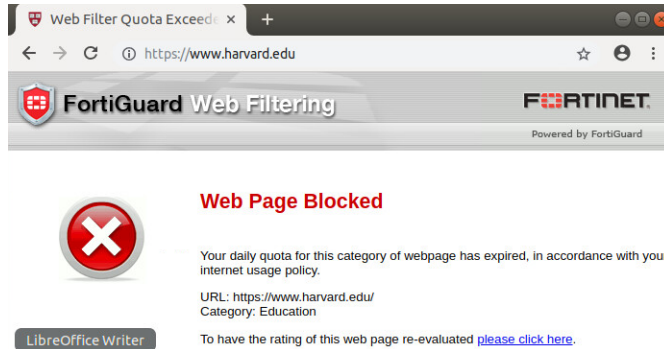
8. Validate the configuration by visiting a website in the education category, for example <https://www.harvard.edu/>. You can view websites in the education category.



9. Check the used and remaining quota in *Monitor > FortiGuard Quota*.

Category Usage Quota		
User	10.1.100.11	
Web Filter Profile	webfilter	
Category	Used Quota	Remaining
Education	1 second(s)	4 minute(s) and 59 second(s)

10. When the quota reaches its limit, traffic is blocked and the replacement page displays.



### To configure a quota in the CLI:

```
config webfilter profile
 edit "webfilter"
 config ftgd-wf
 unset options
 config filters
 edit 1
 set category 30 <-- the id of education category
 next
 end
 config quota
 edit 1
 set category 30
 set type time
 set duration 5m
 next
 end
 end
 next
end
```

## Web content filter

You can control access to web content by blocking web pages containing specific words or patterns. This helps to prevent access to pages with questionable material. You can specify words, phrases, patterns, wildcards and Perl regular expressions to match content on web pages. You can use multiple web content filter lists and select the best web content filter list for each Web Filter profile.

## Pattern type

When you have created the Web Filter content list, you need to add web content patterns to it. There are two types of patterns: wildcard and regular expression.

### Wildcard

Use the wildcard setting to block or exempt one word or text strings of up to 80 characters. You can also use wildcard symbols such as `?` or `*` to represent one or more characters. For example, a wildcard expression *forti\*.com* matches *fortinet.com* and *forticare.com*. The `*` represents any character appearing any number of times.

### Regular expression

Use the regular expression setting to block or exempt patterns of Perl expressions which use some of the same symbols as wildcard expressions but for different purposes. In regular expressions, `*` represents the character before the symbol. For example, *forti\*.com* matches *fortiii.com* but not *fortinet.com* or *fortiice.com*. In this case, the symbol `*` represents *i* appearing any number of times.

The maximum number of web content patterns in a list is 5000.

## Content evaluation

The web content filter feature scans the content of every web page that is accepted by a security policy. The system administrator can specify banned words and phrases and attach a numerical value, or score, to the importance of those words and phrases. When the web content filter scan detects banned content, it adds the scores of banned words and phrases found on that page. If the sum is higher than a threshold set in the Web Filter profile, FortiGate blocks the page.

The default score for web content filter is 10 and the default threshold is 10. This means that by default, a web page is blocked by a single match.

Banned words or phrases are evaluated according to the following rules:

- The score for each word or phrase is counted only once, even if that word or phrase appears many times in the web page.
- The score for any word in a phrase without quotation marks is counted.
- The score for a phrase in quotation marks is counted only if it appears exactly as written.

## Sample of applying banned pattern rules

The following table is an example of how rules are applied to the contents of a web page. For example, a web page contains only this sentence:

*The score for each word or phrase is counted only once, even if that word or phrase appears many times in the web page.*

Banned pattern	Assigned score	Score added to the sum for the entire page	Threshold score	Comment
word	20	20	20	Appears twice but only counted once. Web page is blocked.
word phrase	20	40	20	Each word appears twice but only counted once giving a total score of 40. Web page is blocked.
word sentence	20	20	20	"word" appears twice, "sentence" does not appear, but since any word in a phrase without quotation marks is counted, the score for this pattern is 20. Web page is blocked.
"word sentence"	20	0	20	This phrase does not appear exactly as written. Web page is allowed.
"word or phrase"	20	20	20	This phrase appears twice but is counted only once. Web page is blocked.

## Sample configuration

### To configure web content filter in the GUI:

1. Go to *Security Profiles > Web Filter* and go to the *Static URL Filter* section.
2. Enable *Content Filter* to display its options.

Static URL Filter

Block invalid URLs ☐

URL Filter ☐

Block malicious URLs discovered by FortiSandbox ☐

Content Filter ☒

+ Create New Edit Delete

Pattern Type	Pattern	Language	Action	Status
No results				

3. Select *Create New* to display the content filter options.

Static URL Filter

Block invalid URLs ☐

URL Filter ☐

Block malicious URLs discovered by FortiSandbox ☐

Content Filter ☒

+ Create New Edit Delete

Pattern Type Pattern Language Action Status

No results

New Web Content Filter

Pattern Type Wildcard Regular Expression

Pattern

Language Western

Action Block Exempt

Status Enable Disable

OK Cancel

4. For *Pattern Type*, select *Regular Expression* and enter *fortinet* in the *Pattern* field.

- Leave *Language* as *Western*.
- Set *Action* to *Block*.
- Set *Status* to *Enable*.

New Web Content Filter

Pattern Type: Wildcard **Regular Expression**

Pattern: fortinet

Language: Western

Action: **Block** Exempt

Status: **Enable** Disable

OK Cancel

5. Select *OK* to see the updated *Static URL Filter* section.

Static URL Filter

Block invalid URLs: ☐

URL Filter: ☐

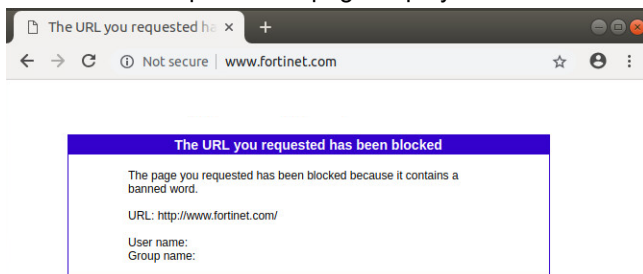
Block malicious URLs discovered by FortiSandbox: ☐

Content Filter: ☒

+ Create New Edit Delete

Pattern Type	Pattern	Language	Action	Status
Regular Expressi...	fortinet	Western	Block	Enable

6. Validate the configuration by visiting a website with the word *fortinet*, for example, [www.fortinet.com](http://www.fortinet.com). The website is blocked and a replacement page displays.



## To configure web content filter in the CLI:

1. Create a content table:

```
config webfilter content
 edit 1 <-- the id of this content
 set name "webfilter"
 config entries
 edit "fortinet" <-- the banned word
 set pattern-type regexp <-- the type is regular expression
 set status enable
 set lang western
 set score 10 <-- the score for this word is 10
 set action block
 next
 end
```

```
 next
end
```

## 2. Attach the content table to the Web Filter profile:

```
config webfilter profile
 edit "webfilter"
 config web
 set bword-threshold 10 <-- the threshold is 10
 set bword-table 1 <-- the id of content table we created in the previous
 step
 end
 config ftgd-wf
 unset options
 end
next
end
```

## File filter

File Filter allows the Web Filter profile to block files passing through a FortiGate based on file type.

HTTP and FTP File Filtering is configurable in Web Filter profile.

File Filtering in Web Filter profile is based on file type (file's meta data) only, and not on file size or file content. You need to configure a DLP sensor to block files based on size or content such as SSN numbers, credit card numbers, or regexp.

File filtering only works on proxy mode policies.

## Supported file types

The following file types are supported in File Filter and DLP profiles:

File Type Name	Description
.net	Match .NET files
7z	Match 7-zip files
activemime	Match activemime files
arj	Match arj compressed files
aspack	Match aspack files
avi	Match avi files
base64	Match base64 files
bat	Match Windows batch files
bin	Match bin files
binhex	Match binhex files
bmp	Match bmp files
bzip	Match bzip files

File Type Name	Description
bzip2	Match bzip2 files
cab	Match Windows cab files
chm	Match Windows compiled HTML help files
class	Match class files
cod	Match cod files
crx	Match Chrome extension files
dmg	Match Apple disk image files
elf	Match elf files
exe	Match Windows executable files
flac	Match FLAC files
fsg	Match fsg files
gif	Match gif files
gzip	Match gzip files
hlp	Match Windows help files
hta	Match hta files
html	Match html files
iso	Match ISO archive files
jad	Match jad files
javascript	Match javascript files
jpeg	Match jpeg files
lzh	Match lzh compressed files
mach-o	Match Mach object files
mime	Match mime files
mov	Match mov files
mp3	Match mp3 files
mpeg	Match mpeg files
msc	Match msc files
msi	Match Windows Installer msi bzip files
msoffice	Match MS-Office files. For example, doc, xls, ppt, and so on.
msofficex	Match MS-Office XML files. For example, docx, xlsx, pptx, and so on.

File Type Name	Description
pdf	Match pdf files
petite	Match petite files
png	Match png files
prc	Match prc files
rar	Match rar archives
rm	Match rm files
sis	Match sis files
tar	Match tar files
tiff	Match tiff files
torrent	Match torrent files
unknown*	Match unknown files
upx	Match upx files
uue	Match uue files
wav	Match wav files
wma	Match wma files
xar	Match xar archive files
xz	Match xz files
zip	Match zip files

\* This file type is only available in DLP profiles.

## Example

In the following example, three file filters are used in the Web Filter profile:

1. Block PDFs from entering our leaving the network (filter1).
2. Log the download of some graphics file-types via HTTP (filter2).
3. Block executable files from leaving to the network over FTP (filter3).

### To configure a file-type based web filter in the CLI:

```
config webfilter profile
 edit "webfilter-file-filter"
 config file-filter
 set status enable
 set log enable
 set scan-archive-contents enable
 config entries
 edit "filter1"
 set comment "Block PDF files"
```

```
 set protocol http ftp
 set action block
 set direction any
 set encryption any
 set file-type "pdf"
 next
 edit "filter2"
 set comment "Log graphics files"
 set protocol http
 set action log
 set direction incoming
 set encryption any
 set file-type "jpeg" "png" "gif"
 next
 edit "filter3"
 set comment "Block upload of EXE files"
 set protocol ftp
 set action block
 set direction outgoing
 set encryption any
 set file-type "exe"
 next
end
end
next
end
```

**After configuring file filters in Web Filter profile, apply it to a firewall policy:**

```
config firewall policy
 edit 1
 set name "client-to-internet"
 set srcintf "dmz"
 set dstintf "wan1"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set utm-status enable
 set utm-inspection-mode proxy
 set logtraffic all
 set webfilter profile "webfilter-filefilter"
 set profile-protocol-options "protocol"
 set ssl-ssh-profile "protocols"
 set nat enable
 next
end
```

### To view the file filter logs:

```
execute log filter category utm-file-filter
execute log display
```

### File filter block action:

```
1: date=2020-06-25 time=10:10:38 logid="1900064000" type="utm" subtype="file-filter"
eventtype="file-filter" level="warning" vd="root" eventtime=1593047438715790048 tz="+0900"
```



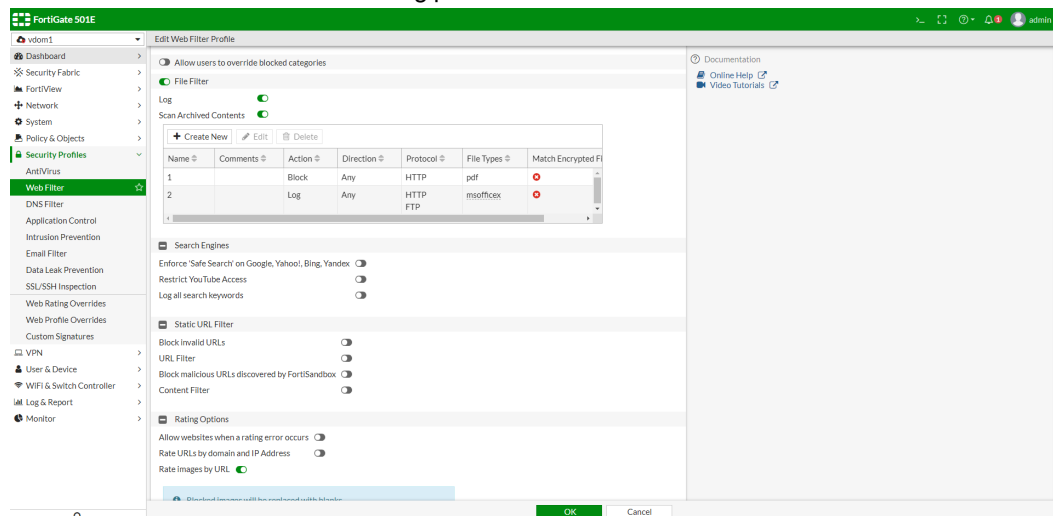
```
policyid=1 sessionid=206159 srcip=10.0.0.20 srcport=46172 srcintf="port1" srcintfrole="lan"
dstip=10.0.10.20 dstport=80 dstintf="wan1" dstintfrole="wan" proto=6 service="HTTP"
profile="default" direction="incoming" action="blocked"
url="http://www.fortitest.jp/download/test.pdf" hostname="www.fortitest.jp"
agent="curl/7.58.0" filtername="test" filename="test.pdf" filesize=17556 filetype="pdf"
msg="File was blocked by file filter."
```

#### File filter log action:

```
2: date=2019-03-19 time=10:48:23 logid="0346012672" type="utm" subtype="file-filter"
eventtype="file-filter" level="notice" vd="vd1" eventtime=1548442102 policyid=1
sessionid=521 srcip=10.1.100.22 srcport=52894 srcintf="dmz" srcintfrole="undefined"
dstip=172.16.200.55 dstport=80 dstintf="wan1" dstintfrole="undefined" proto=6 service="HTTP"
hostname="172.16.200.55" profile="webfilter-filefilter" action="passthrough"
reqtype="direct" url="/app_data/park.jpg" sentbyte=0 rcvdbyte=0 direction="incoming"
filename="park.jpg" filtername="filter2" filetype="jpeg" msg="File was detected by file
filter."
```

#### To configure a file-type based web filter in the GUI:

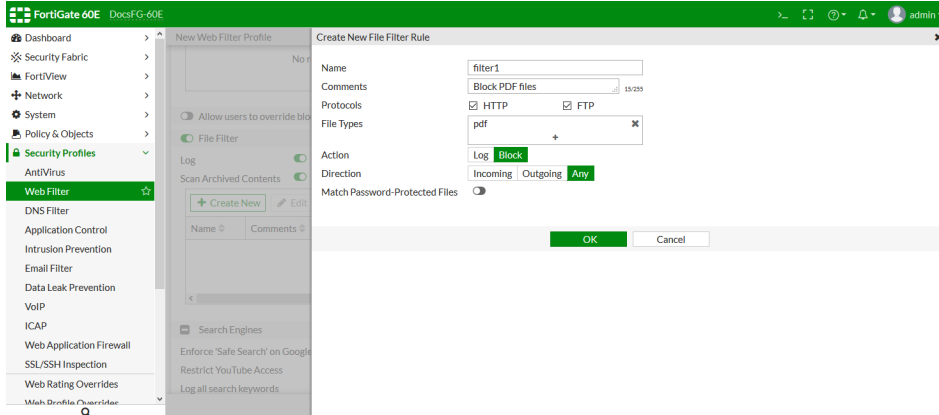
1. Go to *Security Profiles > Web Filter*.
2. Click *Create New* or select an existing profile and click *Edit*.



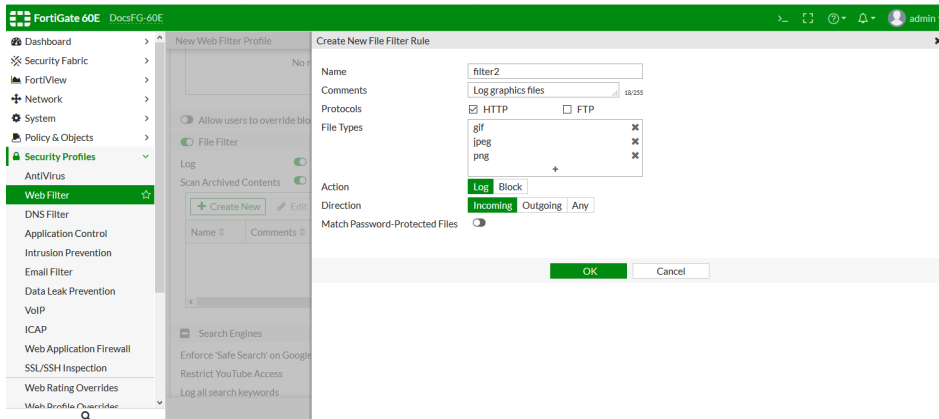
3. Enable *File Filter*.
4. Enable *Log* and *Scan Archived Contents*.
5. In the *File Filter* table, click *Create New*.

## 6. Configure the filters:

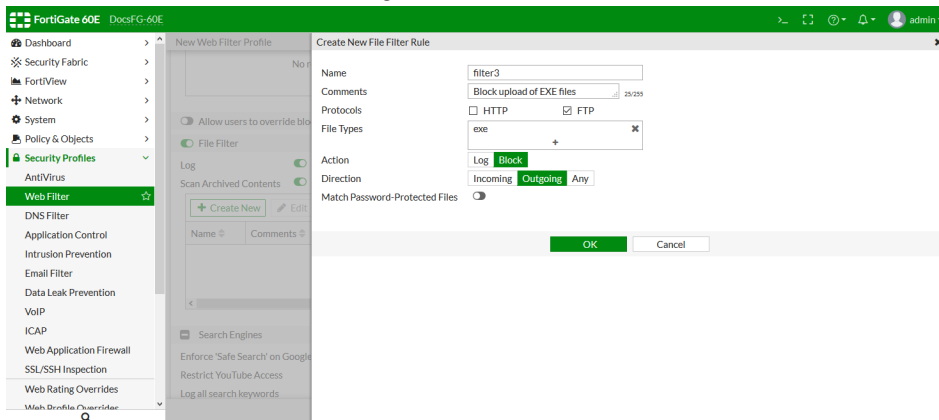
- a. *filter1* blocks PDFs from entering our leaving the network .



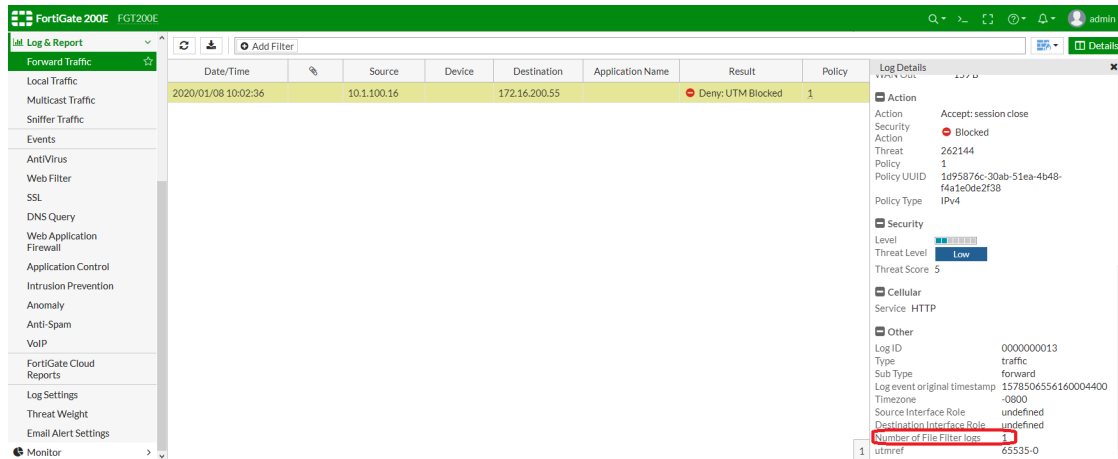
- b. *filter2* logs the download of some graphics file-types via HTTP .



- c. *filter3* blocks EXE files from leaving to the network over FTP .



7. Click **OK**.
8. Add the new web filter profile to a firewall policy.
9. To see if there are file filter logs, go to **VDOM > Log & Report > Forward Traffic**. Select an entry and view the **Log Details**. The number of file filter logs for that entry is listed in the **Other** category.



Date/Time	Source	Device	Destination	Application Name	Result	Policy
2020/01/08 10:02:36	10.1.100.16		172.16.200.55		Deny: UTM Blocked	1

**Log Details**

- Action: Accept: session close
- Security: Blocked
- Action: 262144
- Threat: 1
- Policy: 1
- Policy UUID: 1d95876c-30ab-51ea-4b49-f4a1e0de2f38
- Policy Type: IPv4
- Security:
  - Level: Low
  - Threat Level: Low
  - Threat Score: 5
- Cellular:
  - Service: HTTP
- Other:
  - Log ID: 0000000013
  - Type: traffic
  - Sub-Type: forward
  - Log event original timestamp: 1578506556160004400
  - Timezone: -0800
  - Source Interface Role: undefined
  - Destination Interface Role: undefined
  - Number of File Filter logs: 1



File filter logs can only be viewed in the CLI.

## Advanced filters 1

This topic gives examples of the following advanced filter features:

- Block malicious URLs discovered by FortiSandbox on page 973
- Allow websites when a rating error occurs on page 974
- Rate URLs by domain and IP address on page 974
- Block invalid URLs on page 975
- Rate images by URL on page 976

### Block malicious URLs discovered by FortiSandbox

To use this feature, you must be registered to a FortiSandbox and be connected to it.

This feature blocks malicious URLs that FortiSandbox finds.

For information on configuring FortiSandbox, see [Using FortiSandbox Cloud with antivirus on page 936](#).

**To enable this feature in the GUI:**

1. Go to *Security Profiles > Web Filter* and go to the *Static URL Filter* section.
2. Enable *Block malicious URLs discovered by FortiSandbox*.

**Static URL Filter**

Block invalid URLs ☐

URL Filter ☐

Block malicious URLs discovered by FortiSandbox ☒

Content Filter ☐

**To enable this feature in the CLI:**

```
config webfilter profile
 edit "webfilter"
 config web
 set blacklist enable
 end
 next
end
```

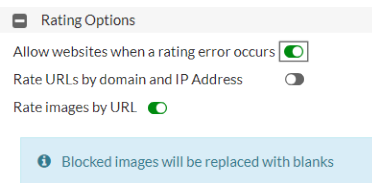
## Allow websites when a rating error occurs

If you don't have a FortiGuard license but you have enabled services that need a FortiGuard license, such as FortiGuard filter, then you'll get a rating error message.

Use this setting to allow access to websites that return a rating error from the FortiGuard Web Filter service.

**To enable this feature in the GUI:**

1. Go to *Security Profiles > Web Filter* and go to the *Rating Options* section.
2. Enable *Allow websites when a rating error occurs*.

**To enable this feature in the CLI:**

```
config webfilter profile
 edit "webfilter"
 config ftgd-wf
 set options error-allow
 end
 next
end
```

## Rate URLs by domain and IP address

If you enable this feature, in addition to only sending domain information to FortiGuard for rating, FortiGate always sends both the URL domain name and the TCP/IP packet's IP address (except for private IP addresses) to FortiGuard for the rating.

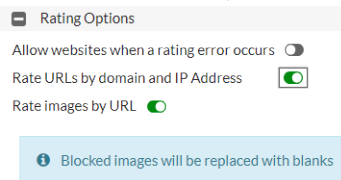
FortiGuard server might return a different category of IP address and URL domain. If they are different, FortiGate uses the rating weight of the IP address or domain name to determine the rating result and decision. This rating weight is hard-coded in FortiGate.

For example, if we use a spoof IP of Google as `www.irs.gov`, FortiGate will send both the IP address and domain name to FortiGuard to get the rating. In this example, we get two different ratings, one is search engine and portals which belongs to the IP of Google, another is government and legal organizations which belongs to `www.irs.gov`. As the search engine

and portals has a higher weight than government and legal organizations, this traffic will be rated as search engine and portals and not rated as government and legal organizations.

### To enable this feature in the GUI:

1. Go to *Security Profiles > Web Filter* and go to the *Rating Options* section.
2. Enable *Rate URLs by domain and IP address*.



### To enable this feature in the CLI:

```
config webfilter profile
 edit "webfilter"
 config ftgd-wf
 set options rate-server-ip
 end
 next
end
```

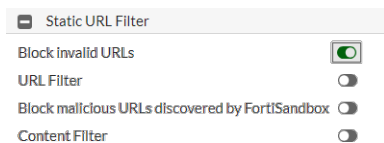
## Block invalid URLs

Use this feature to block websites when their SSL certificate CN field does not contain a valid domain name.

For example, this option blocks URLs which contains spaces. If there is a space in the URL, it must be written as: <http://www.example.com/space%20here.html>.

### To enable this feature in the GUI:

1. Go to *Security Profiles > Web Filter* and go to the *Static URL Filter* section.
2. Enable *Block invalid URLs*.



### To enable this feature in the CLI:

```
config webfilter profile
 edit "webfilter"
 set options block-invalid-url
 next
end
```

## Rate images by URL

This feature enable FortiGate to retrieve ratings for individual images in addition to websites. Images in a blocked category are not displayed even if they are part of a site in an allowed category. Blocked images are replaced with blank placeholders. These image file types are rated: GIF, JPEG, PNG, BMP, and TIFF.

This feature requires a valid FortiGuard license, otherwise rating errors will occur. By default, this feature is enabled.

For example, if the Other Adult Materials category is blocked, before enabling *Rate images by URL*, the image is not blocked:

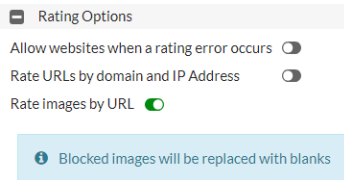


After enabling *Rate images by URL*, images in the Other Adult Materials category are blocked. For example:



**To enable this feature in the GUI:**

1. Go to *Security Profiles > Web Filter* and go to the *Rating Options* section.
2. Enable *Rate images by URL*.

**To enable this feature in the CLI:**

```
config webfilter profile
 edit "webfilter"
 config ftgd-wf
 unset options
 set rate-image-urls enable
 end
 next
end
```

## Advanced filters 2

This topic gives examples of the following advanced filter features:

- [Safe search on page 977](#)
- [YouTube education filters on page 978](#)
  - [Restrict YouTube access on page 978](#)
  - [YouTube channel filtering on page 979](#)
- [Log all search keywords on page 980](#)
- [Restrict Google account usage to specific domains on page 980](#)
- [HTTP POST Action on page 981](#)
- [Remove Java applets, remove ActiveX, and remove cookies on page 982](#)



These advanced filters are only available when inspection mode is *Proxy*.

---

## Safe search

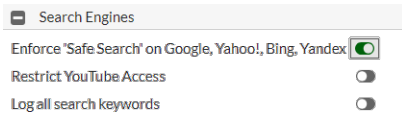
This feature applies to popular search sites and prevents explicit websites and images from appearing in search results.

Supported search sites are:

- Google
- Yahoo
- Bing
- Yandex

**To enable this feature in the GUI:**

1. Go to *Security Profiles > Web Filter* and go to the *Search Engines* section.
2. Enable *Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex*.

**To enable this feature in the CLI:**

```
config webfilter profile
 edit "webfilter"
 config web
 set safe-search url
 end
 next
end
```

**YouTube education filters**

Use these features to limit users' access to YouTube channels, such as in an education environment where you want students and users to be able to access YouTube education videos but not other YouTube videos.

**Restrict YouTube access**

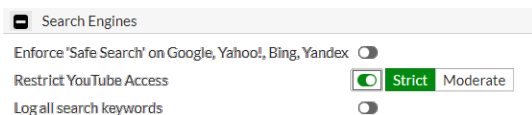
Formerly, YouTube for Schools was a way to access educational videos inside a school network. This YouTube feature lets schools access educational videos on YouTube EDU and to specify the videos accessible within the school network.

When Google stopped supporting YouTube for Schools on July 1, 2016, YouTube safe search also stopped working.

Google provides information on restricting YouTube content such as [Restrict YouTube content available to G Suite users](#). At this time, the options Google offers to restrict inappropriate content includes: DNS, HTTP headers, and Chromebooks..

**To enable this feature in the GUI:**

1. Go to *Security Profiles > Web Filter* and go to the *Search Engines* section.
2. Enable *Restrict YouTube Access* and select *Strict* or *Moderate*.

**To enable this feature in the CLI:**

```
config webfilter profile
 edit "webfilter"
 config web
 set youtube-restrict strict
 end
 next
end
```



## YouTube channel filtering

This Web Filter feature is also called *Restrict YouTube access to specific channels*. Use this feature to block or only allow matching YouTube channels.

The following identifiers are used:

given <channel-id>, affect on:

`www.youtube.com/channel/<channel-id>`

`www.youtube.com/user/<user-id>`

matches channel-id from <meta itemprop="channelId" content="UCGzuuLdQZu9wxDNJHO\_JnA">

`www.youtube.com/watch?v=<string>`

matches channel-id from <meta itemprop="channelId" content="UCGzuuLdQZu9wxDNJHO\_JnA">

### To enable this feature in the GUI:

1. Go to *Security Profiles > Web Filter* and go to the *Proxy Options* section.
2. Enable *Restrict YouTube access to specific channels*.

Proxy Options

Restrict Google account usage to specific domains ☐

Restrict YouTube access to specific channels ☒

Channel ID	Comments	Link
No results		

HTTP POST Action ☒ Allow ☐ Block

Remove Java Applets ☐

Remove ActiveX ☐

Remove Cookies ☐

3. Select *Create New* and specify the *Channel ID*, for example, UCGzuuLdQZu9wxDNJHO\_JnA.

New YouTube Channel Filter

Channel ID

Comments  0/255

4. Select *OK* and the option shows the *Channel ID* and its *Link*.

Proxy Options

Restrict Google account usage to specific domains ☐

Restrict YouTube access to specific channels ☒

Channel ID	Comments	Link
UCGzuuLdQZu9wxDNJHO_JnA		<a href="#">Link</a>

1

### To enable this feature in the CLI:

```
config webfilter profile
edit "webfilter"
```

```
set youtube-channel-status whitelist
config youtube-channel-filter
 edit 1
 set channel-id "UCGzuuiLdQZu9wxDNJHO_JnA"
 next
end
next
end
```

Where:

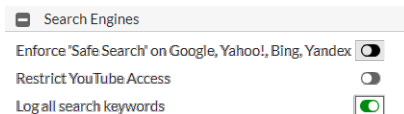
- **whitelist:** only allow the traffic belongs to this channel id and relative identifiers.
- **blacklist:** only block the traffic belongs to this channel id and relative identifiers and allow the other traffic pass

## Log all search keywords

Use this feature to log all search phrases.

**To enable this feature in the GUI:**

1. Go to *Security Profiles > Web Filter* and go to the *Search Engines* section.
2. Enable *Log all search keywords*.



**To enable this feature in the CLI:**

```
config webfilter profile
 edit "webfilter"
 config web
 set log-search enable
 end
 next
end
```

## Restrict Google account usage to specific domains

Use this feature to block access to some Google accounts and services while allowing access to accounts in the domains in the exception list.

**To enable this feature in the GUI:**

1. Go to *Security Profiles > Web Filter* and go to the *Proxy Options* section.
2. Enable *Restrict Google account usage to specific domains*.

Proxy Options

Restrict Google account usage to specific domains ☒

Restrict YouTube access to specific channels ☐

HTTP POST Action Allow Block

Remove Java Applets ☐

Remove ActiveX ☐

Remove Cookies ☐

3. Select the + button and enter the domains that Google can access, for example, `www.fortinet.com`.

Proxy Options

Restrict Google account usage to specific domains ☒

Domain 1

Restrict YouTube access to specific channels ☐

HTTP POST Action Allow Block

When you try to use Google services like Gmail, only traffic from the domain of `www.fortinet.com` can go through. Traffic from other domains is blocked.

## HTTP POST Action

Select the action to take with HTTP POST traffic. HTTP POST is the command used by your browser when you send information, such as a form you have filled-out or a file you are uploading to a web server.

The action options are Allow or Block. The default is Allow.

**To enable this feature in the GUI:**

1. Go to *Security Profiles > Web Filter* and go to the *Proxy Options* section.
2. For *HTTP POST Action*, select *Allow* or *Block*.

Proxy Options

Restrict Google account usage to specific domains ☐

Restrict YouTube access to specific channels ☐

HTTP POST Action Allow Block

Remove Java Applets ☐

Remove ActiveX ☐

Remove Cookies ☐

**To enable this feature in the CLI:**

```
config webfilter profile
 edit "webfilter"
 set post-action [normal/block]
 config ftgd-wf
 unset options
 end
 next
end
```

## Remove Java applets, remove ActiveX, and remove cookies

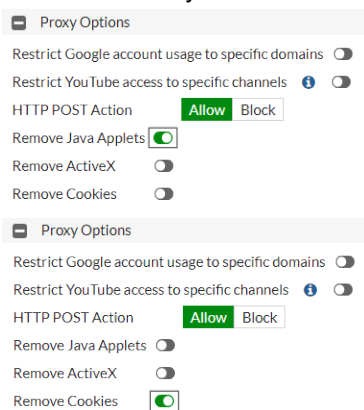
The *Remove Java Applets* feature filters java applets from web traffic. Websites using java applets might not function properly if you enable this filter.

The *Remove ActiveX* feature filters ActiveX scripts from web traffic. Websites using ActiveX might not function properly with if you enable this filter.

The *Remove Cookies* feature filters cookies from web traffic. Websites using cookies might not function properly if you enable this filter.

### To enable this feature in the GUI:

1. Go to *Security Profiles > Web Filter* and go to the *Proxy Options* section.
2. Select the filters you want to use: *Remove Java Applets*, *Remove ActiveX*, and/or *Remove Cookies*.



### To enable this feature in the CLI:

```
config webfilter profile
edit "webfilter"
 set options activexfilter cookiefilter javafilter <-- enable one or more of
activexfilter cookiefilter javafilter.
 config ftgd-wf
 unset options
 end
end
next
end
```

## External resources for web filter

External Resources is a new feature introduced in FortiOS 6.0, which provides a capability to import an external blocklist which sits on an HTTP server. This feature helps FortiGate retrieve a dynamic URL/Domain Name/IP Address/Malware hash list from an external HTTP server periodically. FortiGate uses these external resources as Web Filter's remote categories, DNS Filter's remote categories, policy address objects or antivirus profile's malware definitions. If the external resource is updated, FortiGate objects will update dynamically.

External Resource are categorized into 4 types:

- URL list (Type=*category*)
- Domain Name List (Type=*domain*)

- IP Address list (Type=*address*)
- Malware hash list (Type=*malware*)

For Web Filter profile, it can use category type external resources. Category type external resources file is a URL entries list in a plain text file.

When a *category* type external resource is configured in Web Filter profile, it will be treated as a Remote Category. If the URL in a HTTP/HTTPS request matches the entry inside this external resource file, it will be treated as the Remote Category and follow the action configured for this category in Web Filter profile.

External resource type *category* also can be used in *ssl-ssh-profile* configuration for category-based *SSL-Exempt*. When a Remote Category is configured in *ssl-ssh-profile SSL-Exempt*, if a HTTPS request's URL matches in the Remote Category's entry list, HTTPS request with destination for this URL can be exempted from SSL Deep Inspection.

## External Resources File Format

External Resources File should follow the following requirements:

- The external resource file is a plain text format file and each URL list/IP Address/Domain Name occupies a single line.
- The file is limited to 10M, line is limited 128K (128 x 1024 entries), and the line length limit is 4K characters.
- The entries limited also follow table size limitation defined by CMDB per model.
- The external resource update period can be set to 1 minute, hourly, daily, weekly, or monthly (43200 min, 30 days).
- The external resource type as category (URL list) and domain (Domain Name list) share the category number range 192-221 (total 30 categories).
- There's no duplicated entry validation for external resources file (entry inside each file or inside different files).

For URL list (Type=*category*):

Scheme is optional, and will be truncated if found (*http://*, *https://* is not needed).

Wildcard (\*) is supported (from 6.2). It supports the *\*\*\** at beginning and ending of URL, and not in the middle of URL as follows:

```
+ support *.domain2.com, domain.com.* + not support: domain3.*.com
```

IDN (International Domain Name) and UTF encoding URL is supported (from 6.2).

IPv4,IPv6 format URL is supported. IPv6 in URL list must in *[ ]* form.

## Configure External Resources from CLI

We can use CLI to configure the external resources files that is located on external HTTP Server. Under Global, configure the external resource file location and specify the resource type.

Web Filter will use *category* type external resources as Remote Categories. In the following example, it is configured a file *Ext-Resource-Type-as-Category-1.txt* as type as category, it will be treated in Web Filter as Remote Category, the category name configured as *Ext-Resource-Type-as-Category-1* and category-id as *192*:

```
config system external-resource
 edit "Ext-Resource-Type-as-Category-1"
 set type category <----
 set category 192 <----
 set resource "http://172.16.200.66/external-resources/Ext-Resource-Type-as-Category-1.txt"
 set refresh-rate 1
```

```
 next
end
```

Now in each VDOM, category type external resource can be used in Web Filter as Remote Category. In the example above, URL list in "Ext-Resource-Type-as-Category-1.txt" file will be treated as remote category (category-id 192). Configure the action for this remote category in Web Filter profile and apply it in the policy:

```
config webfilter profile
 edit "webfilter"
 config ftgd-wf
 unset options
 config filters
 edit 1
 set category 2
 set action warning
 next

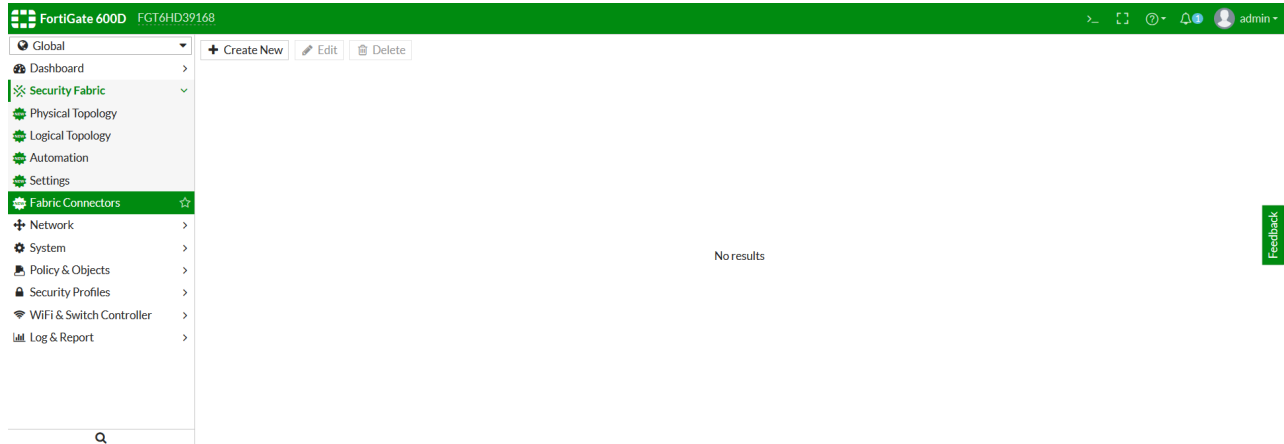
 edit 24
 set category 192 <----
 set action block
 next
 edit 25
 set category 221
 set action warning
 next
 edit 26
 set category 193
 next
 end
 end
 set log-all-url enable
 next
end

config firewall policy
 edit 1
 set name "WebFilter"
 set srcintf "port10"
 set dstintf "port9"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set utm-status enable
 set logtraffic all
 set webfilter-profile "webfilter"
 set profile-protocol-options "protocol"
 set ssl-ssh-profile "protocols"
 set nat enable
 next
end
```

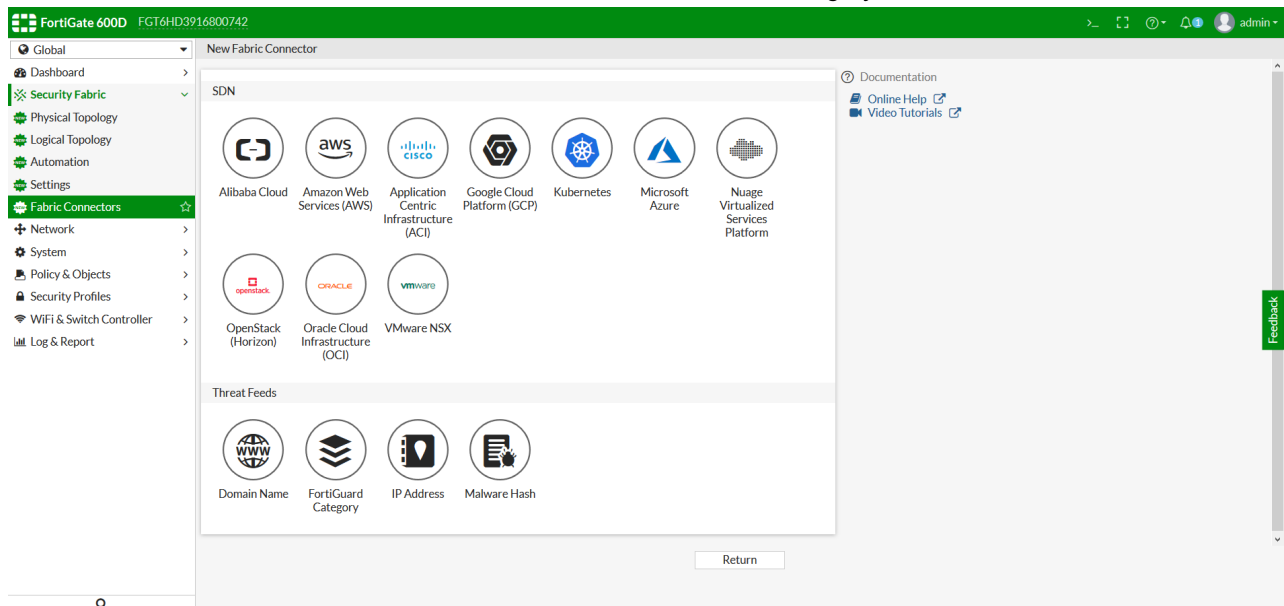
## Configure External Resources from GUI

To configure, edit, or view the Entries for external resources from GUI:

1. Go to *Global > Security Fabric > Fabric Connectors*:



2. Go to *Global > Security Fabric > Fabric Connectors*.
3. Click *Create New*, and in the *Threat Feeds* section, select *FortiGuard Category*.



4. Enter the resource name, URI location of the resource file, resource authentication credential, and *Refresh Rate*.

FortiGate 600D FGT600D.DNS-NAT interim build0810 admin

Global Edit Fabric Connector

Threat Feeds

FortiGuard Category

Connector Settings

Name Ext-Resource-Type-as-Category-1

URI of external resource http://172.16.200.66/external-resource

HTTP basic authentication

Refresh Rate 1

Comments

Last Update 2019/01/17 16:08:08 View Entries

Status On

OK Cancel

5. Click **OK**.
6. After a few minutes, double-click the *Threat Feeds Object* you just configured. It is shown in the *Edit* page.
7. Click **View Entries** to view the entry list in the external resources file:

FortiGate 600D FGT600D.DNS-NAT interim build0810 admin

Global Edit Fabric Connector

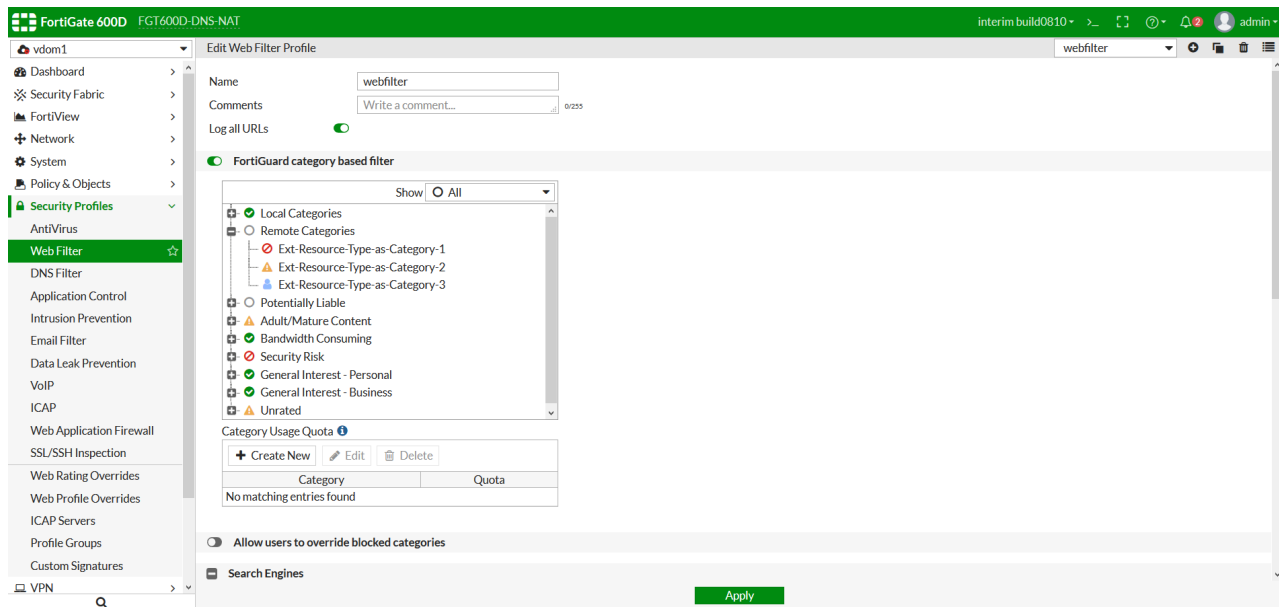
FortiGuard Category Threat Feed "Ext-Resource-Type-as-Category-1"

Search

Entry	Validity
www.example.com	Valid
www.fortinet.com	Valid

8. Go to **VDOM > Security Profiles > Web Filter**. The configured external resources is shown and configured in each Web Filter Profile:





## Log Example

If an HTTP/HTTPS request URL is matched in remote category's entry list, it will override its original FortiGuard URL rating and be treated as a remote category.

Go to **VDOM > Log & Report > Web Filter**:

Date/Time	User	Source	Action	URL	Category Description	Initiator	Sent / Received
2019/01/18 15:49:15		10.1.100.18	blocked	www.fortinet.com	Ext-Resource-Type-as-Category-1		752 B / 10.10 kB

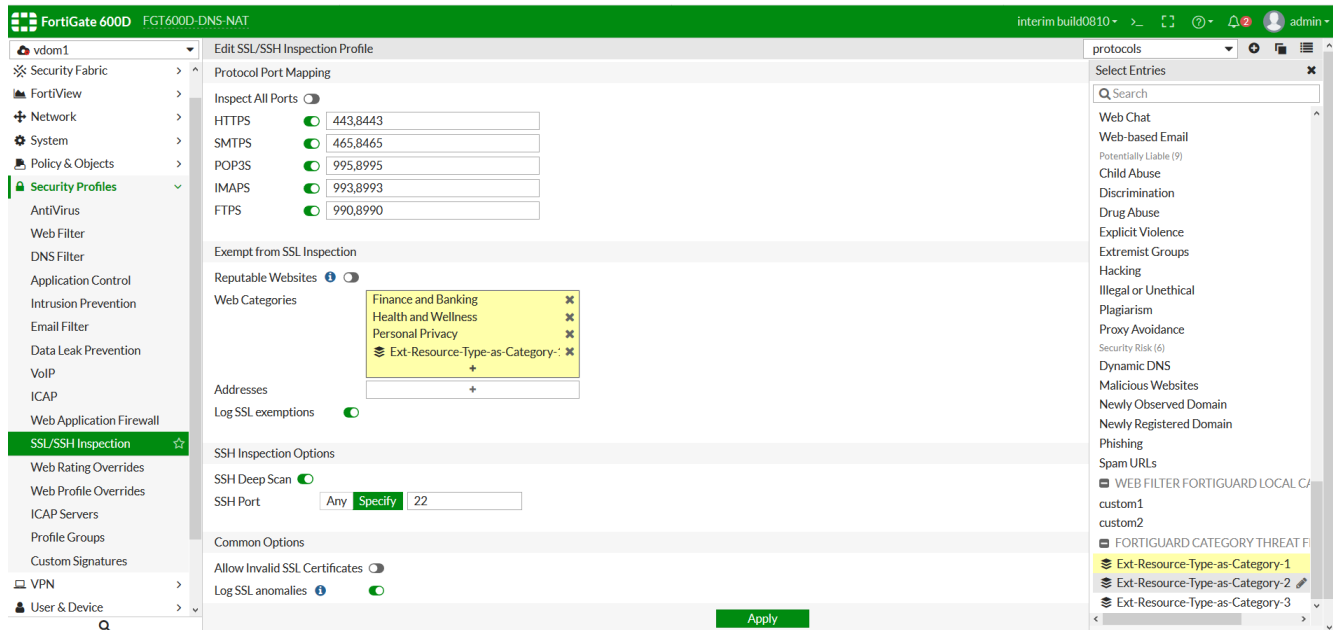
## CLI Example:

```
1: date=2019-01-18 time=15:49:15 logid="0316013056" type="utm" subtype="webfilter"
eventtype="ftgd_blk" level="warning" vd="vdom1" eventtime=1547855353 policyid=1
sessionid=88922 srcip=10.1.100.18 srcport=39886 srcintf="port10" srcintfrole="undefined"
dstip=216.58.193.67 dstport=443 dstintf="port9" dstintfrole="undefined" proto=6
service="HTTPS" hostname="www.fortinet.com" profile="webfilter" action="blocked"
reqtype="direct" url="/" sentbyte=752 rcvbyte=10098 direction="outgoing" msg="URL belongs
to a denied category in policy" method="domain" cat=192 catdesc="Ext-Resource-Type-as-
Category-1"
```

## Remote Category in ssl-ssh-profile category-based SSL-Exempt

Remote category can be applied in *ssl-ssh-profile category-based SSL-Exempt*.

Go to **VDOM > Security Profiles > SSL/SSH Inspection**:



HTTPS request URLs matched in this remote category will be exempted from SSL deep inspection.

### Log example:

```
3: date=2019-01-18 time=16:06:21 logid="0345012688" type="utm" subtype="webfilter"
eventtype="ssl-exempt" level="information" vd="vdom1" eventtime=1547856379 policyid=1
sessionid=90080 srcip=10.1.100.18 srcport=39942 srcintf="port10" srcintfrole="undefined"
dstip=216.58.193.67 dstport=443 dstintf="port9" dstintfrole="undefined" proto=6
service="HTTPS" hostname="www.fortinet.com" profile="webfilter" action="passthrough"
reqtype="direct" url="/" sentbyte=517 rcvbyte=0 direction="outgoing" msg="The SSL session
was exempted." method="domain" cat=192 catdesc="Ext-Resource-Type-as-Category-1"
urlsource="exempt_type_user_cat"
```

## Local Category and Remote Category Priority

Web Filter can have both local category and remote category at the same time. There's no duplication check between local category URL override and remote category resource file. For example, a URL like `www.example.com` may be shown both in remote category entry list and in FortiGate's local category URL override configuration. We recommend avoiding this scenario since FortiGate does not check for duplicates. However, if a URL is duplicated in both local category and remote category, it is rated as local category.

## Reliable web filter statistics

FortiOS 6.2 provides command line tools to view the Web Filter statistics report. These command line tools currently fall into either proxy-based or flow-based Web Filter statistics commands.

## Proxy-based Web Filter statistics report

- The proxy-based Web Filter statistics command line tools are as follows. These commands are available in both global or per-VDOM command lines.

```
#diagnose wad filter <----define the interested objects for output
(global) # diagnose wad ?
console-log Send WAD log messages to the console.
debug Debug setting.
stats Show statistics.
filter Filter for listing sessions or tunnels. <----use filter to filter-out
interested object and output
kxp SSL KXP diagnostics.
user User diagnostics.
memory WAD memory diagnostics.
restore Restore configuration defaults.
history Statistics history.
session Session diagnostics.
tunnel Tunnel diagnostics.
webcache Web cache statistics.
worker Worker diagnostics.
csvc Cache service diagnostics.

#diagnose wad stat filter list/clear <----list/clear Web Filter/DLP statistics
report
```

- In the example below, there are two VDOMs using proxy-based policies which have Web Filter profiles enabled. The command line can be used to view the proxy-based Web Filter statistics report.

```
(global) # diagnose wad filter ?
list Display current filter.
clear Erase current filter settings.
src Source address range to filter by.
dst Destination address range to filter by.
sport Source port range to filter by.
dport Destination port range to filter by.
vd Virtual Domain Name. <----filter for per-vdom or global
statistics report
explicit-policy Index of explicit-policy. -1 matches all.
firewall-policy Index of firewall-policy. -1 matches all.
drop-unknown-session Enable drop message unknown sessions.
negate Negate the specified filter parameter.
protocol Select protocols to filter by.

FGT_600D-ICAP-NAT (global) # diagnose wad filter vd
<vdom> Virtual Domain Name.
ALL all vdoms
root vdom
vdom1 vdom

FGT_600D-ICAP-NAT (global) # diagnose wad filter vd root <----filter-out root vdom
statistics
Drop_unknown_session is enabled.

FGT_600D-ICAP-NAT (global) # diagnose wad stats filter list
filtering of vdom root <----Displayed the WF statistics for root vdom
 dlp = 0 <----Number of Reuquest that DLP Sensor processed;
```

```

content-type = 0 <----Number of Request that matching content-type filter;
urls:
 examined = 6 <----Number of Request that Proxy Web-Filter(all wad daemons)
examined;
 allowed = 3 <----Number of Request that be allowed in the examined requests;
 blocked = 0 <----Number of Request that be blocked in the examined requests;
 logged = 0 <----Number of Request that be logged in the examined requests;
 overridden = 0 <----Number of Request that be overridden to another Web Filter
profile in the examined requests;

FGT_600D-ICAP-NAT (global) # diagnose wad filter vd vdom1 <----filter-out vdom1
statistics

FGT_600D-ICAP-NAT (global) # diagnose wad stats filter list
filtering of vdom vdom1 <----Displayed the WF statistics for vdom1
 dlp = 0
 content-type = 0
 urls:
 examined = 13
 allowed = 2
 blocked = 9
 logged = 8
 overridden = 0

FGT_600D-ICAP-NAT (global) # diagnose wad filter vd ALL

FGT_600D-ICAP-NAT (global) # diagnose wad stats filter list
filtering of all accessible vdoms <----global statistics is sum of two VDOMs
 dlp = 0
 content-type = 0
 urls:
 examined = 19
 allowed = 5
 blocked = 9
 logged = 8
 overridden = 0

```

## Flow-based Web Filter statistics report

- The flow-based Web Filter statistics command line tools are as follows. These commands are available in global command lines only.

```
(global) # diagnose test application ipsmonitor
```

IPS Engine Test Usage:

```

1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
6: Submit attack characteristics now
10: IPS queue length
11: Clear IPS queue length
12: IPS L7 socket statistics

```

```

13: IPS session list
14: IPS NTurbo statistics
15: IPSA statistics
18: Display session info cache
19: Clear session info cache
21: Reload FSA malicious URL database
22: Reload whitelist URL database
24: Display Flow AV statistics
25: Reset Flow AV statistics
27: Display Flow urlfilter statistics
28: Reset Flow urlfilter statistics
29: Display global Flow urlfilter statistics <----List the Flow Web Filter
Statistics
30: Reset global Flow urlfilter statistics <----Reset the Flow Web Filter
Statistics
96: Toggle IPS engines watchdog timer
97: Start all IPS engines
98: Stop all IPS engines
99: Restart all IPS engines and monitor

```

- In the example below, there are two VDOMs using flow-based policies which have Web Filter profiles enabled. The command line can be used to view the flow-based Web Filter statistics report.

```

(global) # diagnose test application ipsmonitor 29
Global URLF states:
request: 14 <----Number of Requests that Flow Web-Filter(all ips engines)
received;
response: 14 <----Number of Response that Flow Web-Filter(all ips engines) sent;
pending: 0 <----Number of Requests that under processing at that moment;
request error: 0 <----Number of Request that have error;
response timeout: 0 <----Number of response that ips engine not been received in-
time;
blocked: 12 <----Number of Request that Flow Web-Filter blocked;
allowed: 2 <----Number of Request that Flow Web-Filter allowed;

```

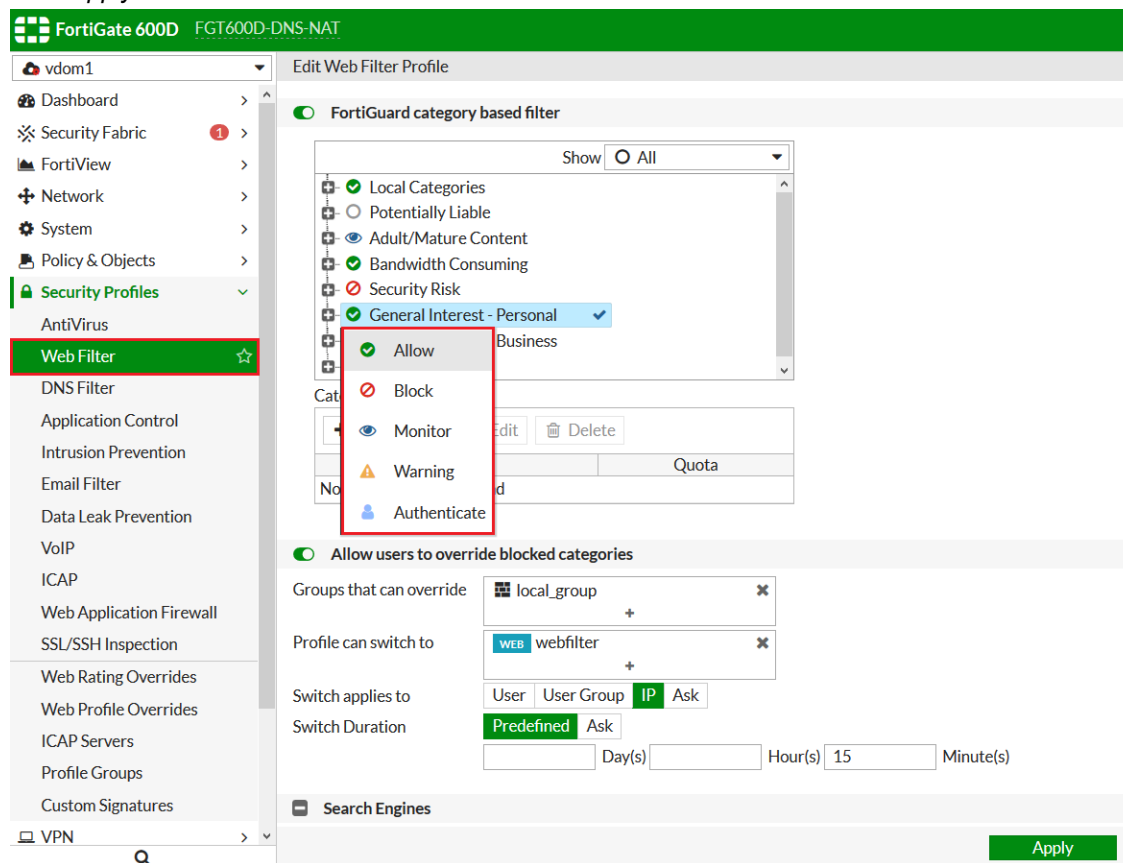
## Flow-based web filtering

Flow-based web filtering includes the following options:

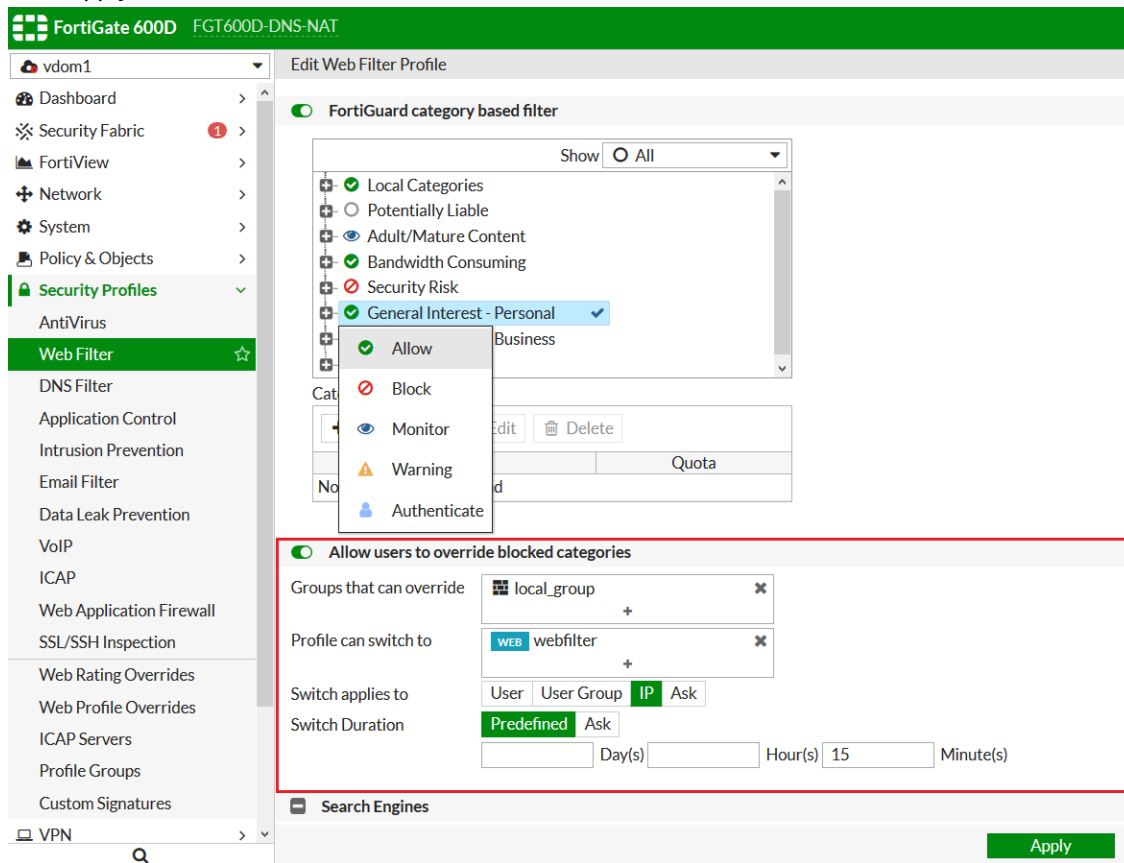
- **Authenticate:** requires user authentication for specific website categories.
- **Warn:** displays a warning message for specific website categories, but allows users to continue to the website.
- **Override:** allows users with valid credentials to override their web filter profile.

**To enable *Authenticate* and *Warning* web filters:**

1. Go to *Security Profiles > Web Filter*.
2. Edit an existing profile, or create a new one.
3. In the *FortiGuard category based filter* section, right-click on a category.
4. Select the *Authenticate* or *Warning* web filter.
5. Configure other settings as needed.

6. Click *Apply*.**To allow users to override blocked categories:**

1. Go to *Security Profiles > Web Filter*.
2. Edit an existing profile, or create a new one.
3. Enable *Allow users to override blocked categories*.
4. Enter information in the following fields:
  - *Groups that can override*
  - *Profile can switch to*
  - *Switch applies to*
  - *Switch Duration*
5. Configure other settings as needed.

6. Click *Apply*.

## URL certificate blacklist

As increasing numbers of malware have started to use SSL to attempt to bypass IPS, maintaining a fingerprint-based certificate blacklist is useful to block botnet communication that relies on SSL.

This feature adds a dynamic package that is distributed by FortiGuard and is part of the Web Filtering service. It is enabled by default for SSL/SSH profiles, and can be configured using the following CLI commands (highlighted in bold):

```
config vdom
 edit <vdom>
 config firewall ssl-ssh-profile
 edit "certificate-inspection"
 set comment "Read-only SSL handshake inspection profile."
 config ssl
 set inspect-all disable
 end
 config https
 set ports 443
 set status certificate-inspection
 set invalid-server-cert block
 set untrusted-server-cert allow
 set sni-server-cert-check enable
 end
 config ftps
```

```
 set status disable
 set invalid-server-cert block
 set untrusted-server-cert allow
 end
 config imaps
 set status disable
 set invalid-server-cert block
 set untrusted-server-cert allow
 end
 config pop3s
 set status disable
 set invalid-server-cert block
 set untrusted-server-cert allow
 end
 config smtps
 set status disable
 set invalid-server-cert block
 set untrusted-server-cert allow
 end
 config ssh
 set ports 22
 set status disable
 set inspect-all disable
 set unsupported-version bypass
 set ssh-tun-policy-check disable
 set ssh-algorithm compatible
 end
 set block-blacklisted-certificates enable
 set caname "Fortinet_CA_SSL"
 set ssl-anomalies-log enable
next
edit "deep-inspection"
 set comment "Read-only deep inspection profile."
 config ssl
 set inspect-all disable
 end
 config https
 set ports 443
 set status deep-inspection
 set client-cert-request bypass
 set unsupported-ssl bypass
 set invalid-server-cert block
 set untrusted-server-cert allow
 set sni-server-cert-check enable
 end
 config ftps
 set ports 990
 set status deep-inspection
 set client-cert-request bypass
 set unsupported-ssl bypass
 set invalid-server-cert block
 set untrusted-server-cert allow
 end
 config imaps
 set ports 993
 set status deep-inspection
```



```
 set client-cert-request inspect
 set unsupported-ssl bypass
 set invalid-server-cert block
 set untrusted-server-cert allow
 end
 config pop3s
 set ports 995
 set status deep-inspection
 set client-cert-request inspect
 set unsupported-ssl bypass
 set invalid-server-cert block
 set untrusted-server-cert allow
 end
 config smtps
 set ports 465
 set status deep-inspection
 set client-cert-request inspect
 set unsupported-ssl bypass
 set invalid-server-cert block
 set untrusted-server-cert allow
 end
 config ssh
 set ports 22
 set status disable
 set inspect-all disable
 set unsupported-version bypass
 set ssh-tun-policy-check disable
 set ssh-algorithm compatible
 end
 set whitelist disable
 set block-blacklisted-certificates enable
 config ssl-exempt
 edit 1
 set type fortiguard-category
 set fortiguard-category 31
 next
 edit 2
 set type fortiguard-category
 set fortiguard-category 33
 next
 edit 3
 set type wildcard-fqdn
 set wildcard-fqdn "g-adobe"
 next
 edit 4
 set type wildcard-fqdn
 set wildcard-fqdn "g-Adobe Login"
 next
 edit 5
 set type wildcard-fqdn
 set wildcard-fqdn "g-android"
 next
 edit 6
 set type wildcard-fqdn
 set wildcard-fqdn "g-apple"
 next
 end
```

```
edit 7
 set type wildcard-fqdn
 set wildcard-fqdn "g-appstore"
next
edit 8
 set type wildcard-fqdn
 set wildcard-fqdn "g-auth.gfx.ms"
next
edit 9
 set type wildcard-fqdn
 set wildcard-fqdn "g-citrix"
next
edit 10
 set type wildcard-fqdn
 set wildcard-fqdn "g-dropbox.com"
next
edit 11
 set type wildcard-fqdn
 set wildcard-fqdn "g-eease"
next
edit 12
 set type wildcard-fqdn
 set wildcard-fqdn "g-firefox update server"
next
edit 13
 set type wildcard-fqdn
 set wildcard-fqdn "g-fortinet"
next
edit 14
 set type wildcard-fqdn
 set wildcard-fqdn "g-googleapis.com"
next
edit 15
 set type wildcard-fqdn
 set wildcard-fqdn "g-google-drive"
next
edit 16
 set type wildcard-fqdn
 set wildcard-fqdn "g-google-play2"
next
edit 17
 set type wildcard-fqdn
 set wildcard-fqdn "g-google-play3"
next
edit 18
 set type wildcard-fqdn
 set wildcard-fqdn "g-Gotomeeting"
next
edit 19
 set type wildcard-fqdn
 set wildcard-fqdn "g-icloud"
next
edit 20
 set type wildcard-fqdn
 set wildcard-fqdn "g-itunes"
next
```

```
 edit 21
 set type wildcard-fqdn
 set wildcard-fqdn "g-microsoft"
 next
 edit 22
 set type wildcard-fqdn
 set wildcard-fqdn "g-skype"
 next
 edit 23
 set type wildcard-fqdn
 set wildcard-fqdn "g-softwareupdate.vmware.com"
 next
 edit 24
 set type wildcard-fqdn
 set wildcard-fqdn "g-verisign"
 next
 edit 25
 set type wildcard-fqdn
 set wildcard-fqdn "g-Windows update 2"
 next
 edit 26
 set type wildcard-fqdn
 set wildcard-fqdn "g-live.com"
 next
 edit 27
 set type wildcard-fqdn
 set wildcard-fqdn "g-google-play"
 next
 edit 28
 set type wildcard-fqdn
 set wildcard-fqdn "g-update.microsoft.com"
 next
 edit 29
 set type wildcard-fqdn
 set wildcard-fqdn "g-swscan.apple.com"
 next
 edit 30
 set type wildcard-fqdn
 set wildcard-fqdn "g-autoupdate.opera.com"
 next
 end
 set server-cert-mode re-sign
 set caname "Fortinet_CA_SSL"
 set untrusted-caname "Fortinet_CA_Untrusted"
 set ssl-anomalies-log enable
 set ssl-exemptions-log disable
 set rpc-over-https disable
 set mapi-over-https disable
 set use-ssl-server disable
next
end
next
end
```

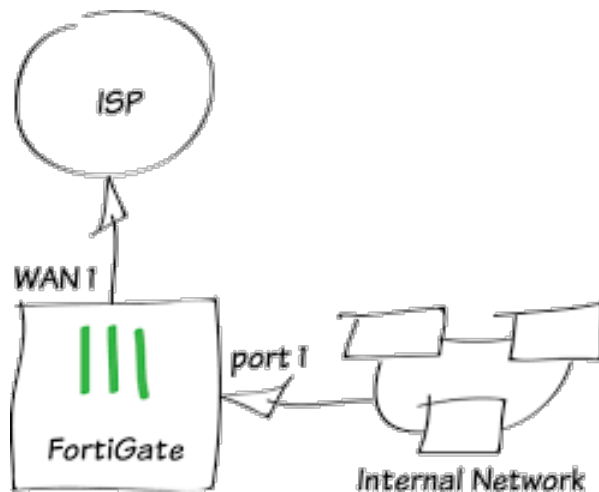
## DNS filter

You can apply DNS category filtering to control user access to web resources. You can customize the default profile, or create your own to manage network user access and apply it to a firewall policy, or you can add it to a DNS server on a FortiGate interface.

DNS filtering has the following features:

- FortiGuard Filtering: filters the DNS request based on the FortiGuard domain rating.
- Botnet C&C domain blocking: blocks the DNS request for the known botnet C&C domains.
- External dynamic category domain filtering: allows you to define your own domain category.
- DNS safe search: enforces Google, Bing, and YouTube safe addresses for parental controls.
- Local domain filter: allows you to define your own domain list to block or allow.
- External IP block list: allows you to define an IP block list to block resolved IPs that match this list.
- DNS translation: maps the resolved result to another IP that you define.

The following sample topology is used in the topics of this section. It includes an internal network and a FortiGate that is used as a gateway device that all DNS traffic traverses.



Some features of this functionality require a subscription to FortiGuard Web Filtering.

## DNS filter behavior in proxy mode

In cases where the DNS proxy daemon handles the DNS filter and if DNS caching is enabled (this is the default setting), then the FortiGate will respond to subsequent DNS queries using the result in the DNS cache and will not forward these queries to a real DNS server.

There are two options to disable this behavior:

- Disable DNS caching globally.
- Remove the DNS filter profile from the proxy mode firewall policy or from the DNS server configured on a FortiGate interface.

### To disable DNS caching globally:

```
config system dns
 set dns-cache-limit 0
end
```



There will be a performance impact to DNS queries since each query will not be cached, and will be forwarded to a real DNS server.

---

The following topics provide information about DNS filters:

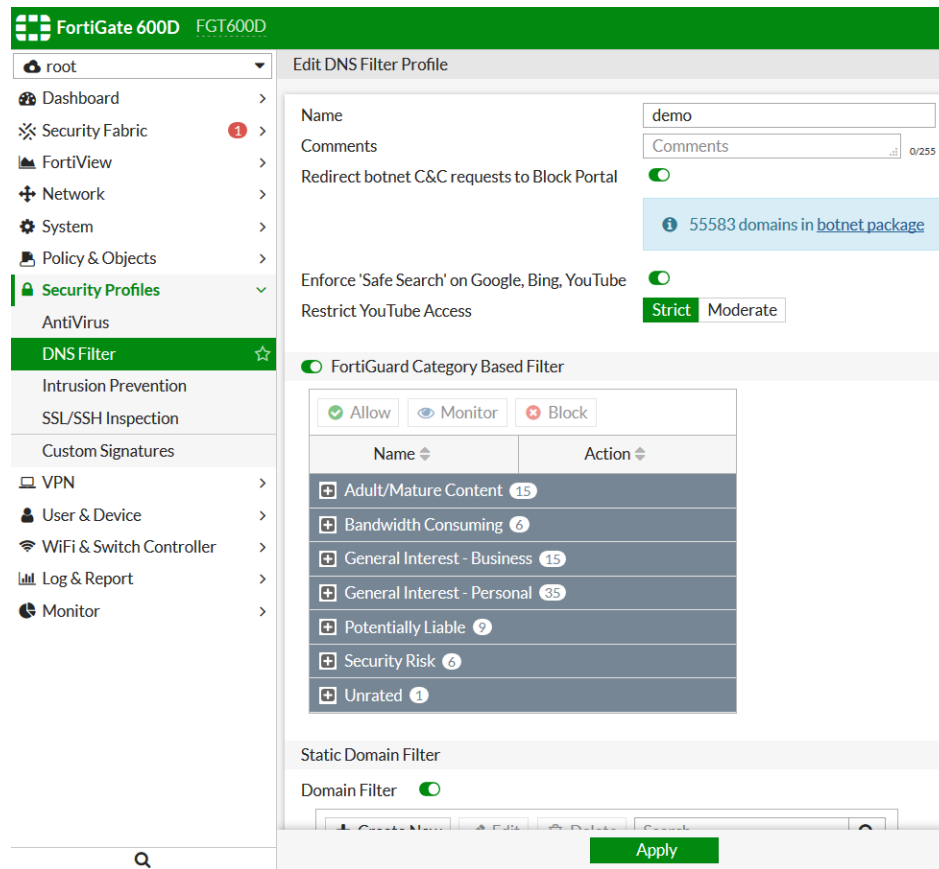
- [How to configure and apply a DNS filter profile on page 999](#)
- [FortiGuard category-based DNS domain filtering on page 1002](#)
- [Botnet C&C domain blocking on page 1006](#)
- [DNS safe search on page 1009](#)
- [Local domain filter on page 1011](#)
- [DNS translation on page 1014](#)
- [Using a FortiGate as a DNS server on page 1017](#)
- [Troubleshooting for DNS filter on page 1018](#)

## How to configure and apply a DNS filter profile

### To create or configure DNS Filter profile in the GUI:

1. Go to *Security Profiles > DNS Filter*.
2. You can modify the default DNS Filter and enable the options you want or you can click + at the top right to create a

new DNS Filter.



### To create or configure DNS Filter profile in the CLI:

```
config dnsfilter profile
 edit "demo"
 set comment ''
 config domain-filter
 unset domain-filter-table
 end
 config ftgd-dns
 set options error-allow
 config filters
 edit 2
 set category 2
 set action monitor
 next
 edit 7
 set category 7
 set action block
 next
 ...
 edit 22
 set category 0
 set action monitor
 next
 end
 end
 end
```

```

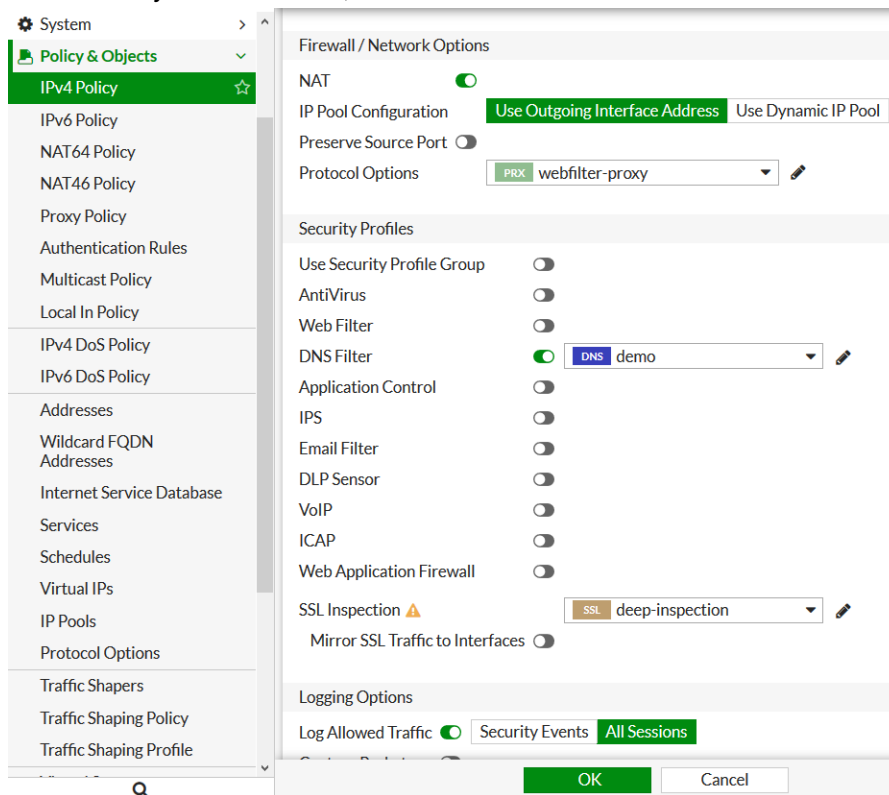
end
set log-all-domain enable
set sdns-ftgd-err-log enable
set sdns-domain-log enable
set block-action redirect
set block-botnet enable
set safe-search enable
set redirect-portal 93.184.216.34
set redirect-portal6 ::
set youtube-restrict strict
next
end

```

After you have created the DNS Filter profile, you can apply it to the policy. DNS filters also support IPv6 policies.

### To apply DNS Filter profile to the policy in the GUI:

1. Go to *Policy & Objects IPv4 Policy* or *IPv6 Policy*.
2. In the *Security Profiles* section, enable *DNS Filter* and select the DNS filter.



### To apply DNS Filter profile to the policy in the CLI:

```

config firewall policy
edit 1
set name "Demo"
set srcintf "port10"
set dstintf "port9"
set srcaddr "all"
set dstaddr "all"

```

```
set action accept
set schedule "always"
set service "ALL"
set utm-status enable
set inspection-mode proxy
set logtraffic all
set fsso disable
set dnsfilter-profile "demo" <<<====
set profile-protocol-options "default"
set ssl-ssh-profile "deep-inspection"
set nat enable

next
end
```

## DNS filter behavior in proxy mode

In cases where the DNS proxy daemon handles the DNS filter and if DNS caching is enabled (this is the default setting), then the FortiGate will respond to subsequent DNS queries using the result in the DNS cache and will not forward these queries to a real DNS server.

There are two options to disable this behavior:

- Disable DNS caching globally.
- Remove the DNS filter profile from the proxy mode firewall policy or from the DNS server configured on a FortiGate interface.

### To disable DNS caching globally:

```
config system dns
 set dns-cache-limit 0
end
```



There will be a performance impact to DNS queries since each query will not be cached, and will be forwarded to a real DNS server.

---

## FortiGuard category-based DNS domain filtering



The FortiGate must have a FortiGuard Web Filter license to use FortiGuard Category Based Filter.

---

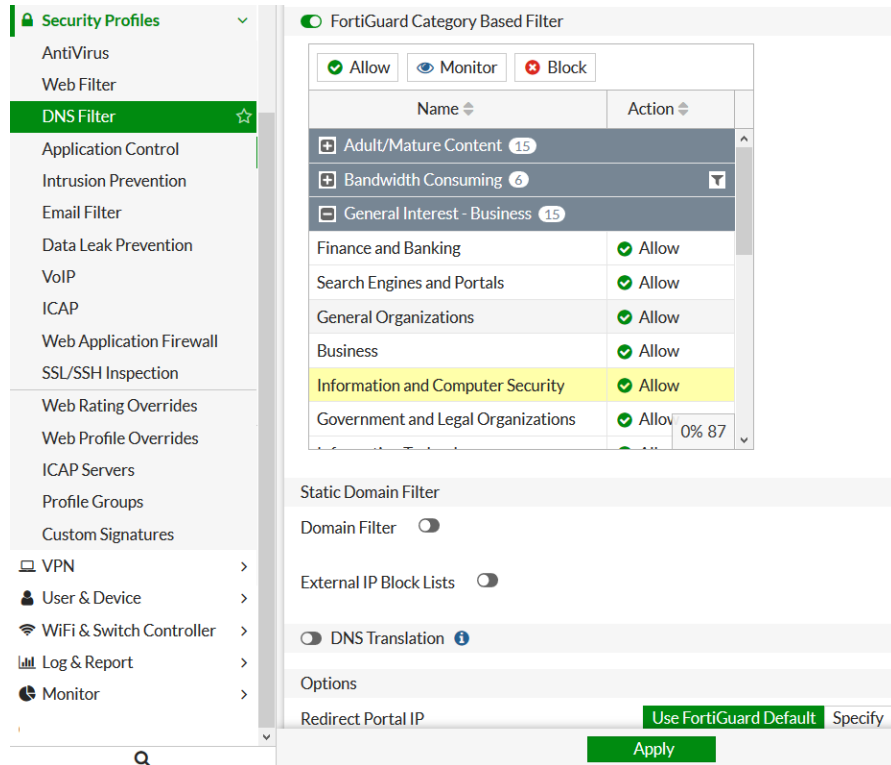
You can use the FortiGuard category-based DNS Domain Filter to inspect DNS traffic. This makes use of FortiGuard's continually updated domain rating database for more reliable protection.

### To configure FortiGuard category-based DNS Domain Filter by GUI:

1. Go to *Security Profiles > DNS Filter* and edit or create a DNS Filter.
2. Enable *FortiGuard Category Based Filter*.

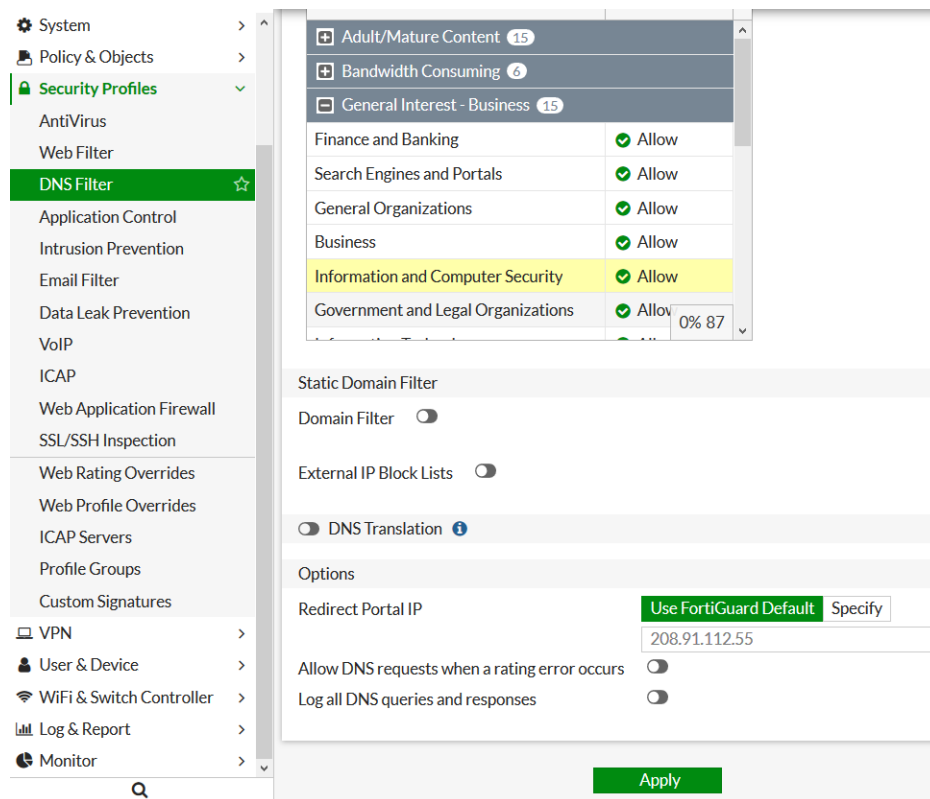


3. Select the category and then select *Allow*, *Monitor*, or *Block* for that category.



4. If you select *Block*, there are two options:

- *Redirect Portal IP*. If the DNS query domain will be blocked, FortiGate will use portal IP to replace the resolved IP in DNS response packet. You can use the default portal IP 208.91.112.55 or click *Specify* to enter another portal IP.
- *Block*. Blocked DNS query has no response return and the DNS query client will time out.



### To configure FortiGuard category-based DNS Domain Filter by CLI:

```
config dnsfilter profile
edit "demo"
 set comment ''
 config domain-filter
 unset domain-filter-table
 end
 config ftgd-dns
 set options error-allow
 config filters <<===== FortiGuard Category Based Filter
 edit 2
 set category 2
 set action monitor
 next
 edit 7
 set category 7
 set action monitor
 next
 ...
 edit 22
 set category 0
 set action monitor
 next
 end
 end
 set log-all-domain enable
 set sdns-ftgd-err-log enable
```

```

 set sdns-domain-log enable
 set block-action redirect/block <<<=== You can specify Block or Redirect
 set block-botnet enable
 set safe-search enable
 set redirect-portal 93.184.216.34 <<<=== Specify Redirect portal-IP.
 set redirect-portal6 ::
 set youtube-restrict strict
 next
end

```

## Sample

To see an example of how this works, from your internal network PC, use a command line tool such as dig or nslookup to do DNS query for some domains, for example:

```

#dig www.example.com
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 61252
;; Flags: qr rd ra; QUERY: 1; ANSWER: 1; AUTHORITY: 13; ADDITIONAL: 11

;; QUESTION SECTION:
;; www.example.com. IN A

;; ANSWER SECTION:
www.example.com. 17164 IN A 93.184.216.34

;; AUTHORITY SECTION:
com. 20027 IN NS h.gtld-servers.net.
com. 20027 IN NS i.gtld-servers.net.
com. 20027 IN NS f.gtld-servers.net.
com. 20027 IN NS d.gtld-servers.net.
com. 20027 IN NS j.gtld-servers.net.
com. 20027 IN NS l.gtld-servers.net.
com. 20027 IN NS e.gtld-servers.net.
com. 20027 IN NS a.gtld-servers.net.
com. 20027 IN NS k.gtld-servers.net.
com. 20027 IN NS g.gtld-servers.net.
com. 20027 IN NS m.gtld-servers.net.
com. 20027 IN NS c.gtld-servers.net.
com. 20027 IN NS b.gtld-servers.net.

;; ADDITIONAL SECTION:
a.gtld-servers.net. 21999 IN A 192.5.6.30
a.gtld-servers.net. 21999 IN AAAA 2001:503:a83e::2:30
b.gtld-servers.net. 21997 IN A 192.33.14.30
b.gtld-servers.net. 21997 IN AAAA 2001:503:231d::2:30
c.gtld-servers.net. 21987 IN A 192.26.92.30
c.gtld-servers.net. 20929 IN AAAA 2001:503:83eb::30
d.gtld-servers.net. 3340 IN A 192.31.80.30
d.gtld-servers.net. 3340 IN AAAA 2001:500:856e::30
e.gtld-servers.net. 19334 IN A 192.12.94.30
e.gtld-servers.net. 19334 IN AAAA 2001:502:1ca1::30
f.gtld-servers.net. 3340 IN A 192.35.51.30

;; Received 509 B
;; Time 2019-04-05 09:39:33 PDT
;; From 172.16.95.16@53(UDP) in 3.8 ms

```

### To check the DNS Filter log in the GUI:

1. Go to **Log & Report > DNS Query** to view the DNS traffic that just traverse the FortiGate and the FortiGuard rating for this domain name.

Date/Time	Sub Type	Source	Domain Name	Query Type	Policy	Message	Domain Filter List	Category	Category Description	Domain Filter Index	#
2019/04/05 09:39:34	dns	10.1.100.18	www.example.com	A	1	Domain is monitored		52	Information Technology		1
2019/04/05 09:39:34	dns	10.1.100.18	www.example.com	A	1						2

### To check the DNS log in the CLI:

```
#execute log filter category utm-dns
```

```
execute log display
2 logs found.
2 logs returned.
```

```
1: date=2019-04-05 time=09:39:34 logid="1501054802" type="utm" subtype="dns" eventtype="dns-response" level="notice" vd="vdom1" eventtime=1554482373 policyid=1 sessionid=50868 srcip=10.1.100.18 srcport=34308 srcintf="port10" srcintfrole="undefined" dstip=172.16.95.16 dstport=53 dstintf="port9" dstintfrole="undefined" proto=17 profile="demo" xid=17647 qname="www.example.com" qtype="A" qtypeval=1 qclass="IN" ipaddr="93.184.216.34" msg="Domain is monitored" action="pass" cat=52 catdesc="Information Technology"

2: date=2019-04-05 time=09:39:34 logid="1500054000" type="utm" subtype="dns" eventtype="dns-query" level="information" vd="vdom1" eventtime=1554482373 policyid=1 sessionid=50868 srcip=10.1.100.18 srcport=34308 srcintf="port10" srcintfrole="undefined" dstip=172.16.95.16 dstport=53 dstintf="port9" dstintfrole="undefined" proto=17 profile="demo" xid=17647 qname="www.example.com" qtype="A" qtypeval=1 qclass="IN"
```

## Botnet C&C domain blocking

FortiGuard Service continually updates the Botnet C&C domain list (Domain DB). The botnet C&C domain blocking feature can block the botnet website access at the DNS name resolving stage. This provides additional protection for your network.

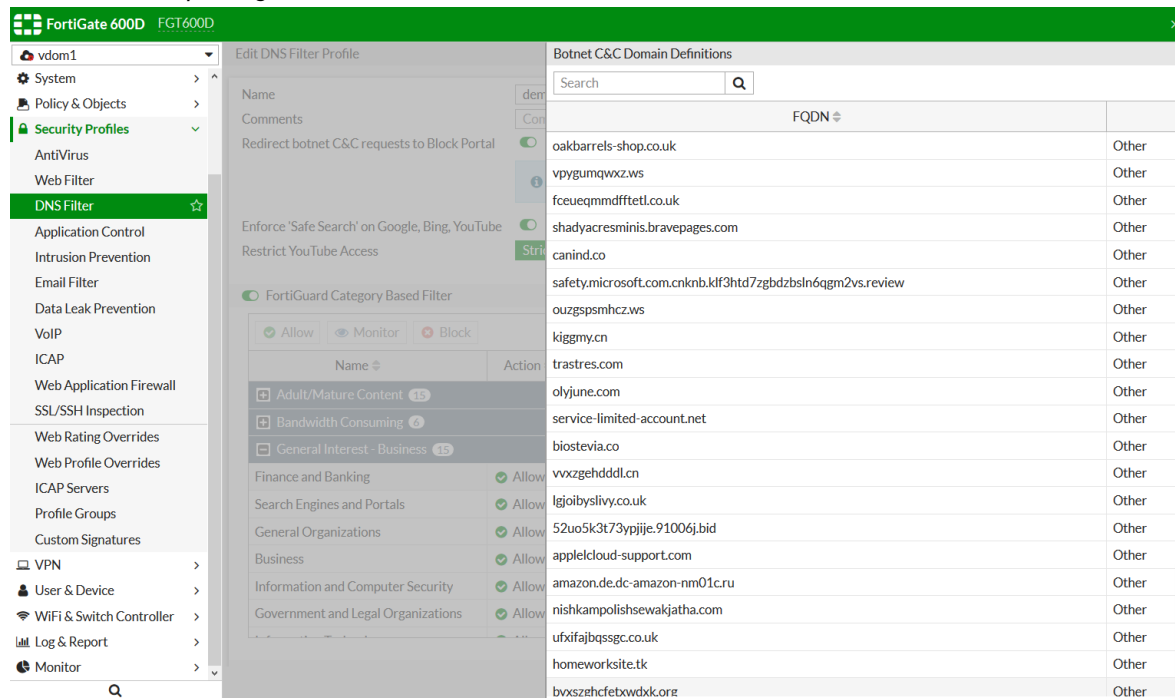
### To configure botnet C&C domain blocking in the GUI:

1. Go to **Security Profiles > DNS Filter** and edit or create a DNS Filter.
2. Enable **Redirect botnet C&C requests to Block Portal**.

Name: demo  
 Comments:   
 Redirect botnet C&C requests to Block Portal: ☒

55583 domains in [botnet package](#)

- Click the *botnet package* link to see the latest botnet C&C domain list.



## Sample

To see an example of how this works, select a botnet domain from that list. Then from your internal network PC, use a command line tool such as dig or nslookup to send a DNS query to traverse the FortiGate to see the query blocked as a botnet domain. For example:

```
#dig canind.co
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 997
;; Flags: qr rd; QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 0

;; QUESTION SECTION:
;; canind.co. IN A

;; ANSWER SECTION:
canind.co. 60 IN A 208.91.112.55 <<<==== botnet domain query
blocked, redirect with portal-IP.

;; Received 43 B
;; Time 2019-04-05 09:55:21 PDT
;; From 172.16.95.16@53 (UDP) in 0.3 ms
```

## To check the DNS Filter log in the GUI:

- Go to *Log & Report > DNS Query* to view the DNS query blocked as a botnet domain.

Events	Date/Time	Sub Type	Source	Domain Name	Query Type	Policy	Message	Domain Filter List	Category	Category Description
AntiVirus	2019/04/04 16:43:59	dns	10.1.100.18	canind.co	A	1	Domain was blocked by dns botnet C&C			
Web Filter	2019/04/04 16:43:59	dns	10.1.100.18	canind.co	A	1				
DNS Query										

**To check the DNS Filter log in the CLI:**

```
(vdom1) # execute log filter category utm-dns

(vdom1) # execute log display
2 logs found.
2 logs returned.

1: date=2019-04-04 time=16:43:59 logid="1501054601" type="utm" subtype="dns" eventtype="dns-
response" level="warning" vd="vdom1" eventtime=1554421439 policyid=1 sessionid=14135
srcip=10.1.100.18 srcport=57447 srcintf="port10" srcintfrole="undefined" dstip=172.16.95.16
dstport=53 dstintf="port9" dstintfrole="undefined" proto=17 profile="demo" xid=24339
qname="canind.co" qtype="A" qtypeval=1 qclass="IN" msg="Domain was blocked by dns botnet
C&C" action="redirect" botnetdomain="canind.co"

2: date=2019-04-04 time=16:43:59 logid="1500054000" type="utm" subtype="dns" eventtype="dns-
query" level="information" vd="vdom1" eventtime=1554421439 policyid=1 sessionid=14135
srcip=10.1.100.18 srcport=57447 srcintf="port10" srcintfrole="undefined" dstip=172.16.95.16
dstport=53 dstintf="port9" dstintfrole="undefined" proto=17 profile="demo" xid=24339
qname="canind.co" qtype="A" qtypeval=1 qclass="IN"
```

**Botnet C&C IPDB blocking**

FortiGate also maintains a botnet C&C IP address database (botnet IPDB). If a DNS query response IP address (resolved IP address) matches an entry inside the botnet IPDB, this DNS query is also blocked by DNS Filter botnet C&C blocking.

**To view the botnet IPDB list in the CLI:**

```
(global) # diagnose sys botnet list 9000 10
9000. proto=TCP ip=103.228.28.166, port=80, rule_id=7630075, name_id=3, hits=0
9001. proto=TCP ip=5.9.32.166, port=481, rule_id=4146631, name_id=7, hits=0
9002. proto=TCP ip=91.89.44.166, port=80, rule_id=48, name_id=96, hits=0
9003. proto=TCP ip=46.211.46.166, port=80, rule_id=48, name_id=96, hits=0
9004. proto=TCP ip=77.52.52.166, port=80, rule_id=48, name_id=96, hits=0
9005. proto=TCP ip=98.25.53.166, port=80, rule_id=48, name_id=96, hits=0
9006. proto=TCP ip=70.120.67.166, port=80, rule_id=48, name_id=96, hits=0
9007. proto=TCP ip=85.253.77.166, port=80, rule_id=48, name_id=96, hits=0
9008. proto=TCP ip=193.106.81.166, port=80, rule_id=48, name_id=96, hits=0
9009. proto=TCP ip=58.13.84.166, port=80, rule_id=48, name_id=96, hits=0
```

To see an example of how DNS Filter botnet C&C IPDB blocking works, select an IP address from the IPDB list and use Internet reverse lookup service to find its corresponding domain name. Then from your internal network PC, use a command line tool such as dig or nslookup to query this domain and see that it's blocked by DNS Filter botnet C&C blocking. For example:

```
dig cpe-98-25-53-166.sc.res.rr.com
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 35135
;; Flags: qr rd; QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 0

;; QUESTION SECTION:
;; cpe-98-25-53-166.sc.res.rr.com. IN A

;; ANSWER SECTION:
cpe-98-25-53-166.sc.res.rr.com. 60 IN A 208.91.112.55 <<<==== Since
```

resolved IP address match the botnet IPDB, dns query blocked with redirect portal IP.

```
;; Received 64 B
;; Time 2019-04-05 11:06:47 PDT
;; From 172.16.95.16@53 (UDP) in 0.6 ms
```

### To check the DNS Filter log in the GUI:

1. Go to **Log & Report > DNS Query** to view the DNS query blocked by botnet C&C IPDB blocking.

Date/Time	Sub Type	Source	Domain Name	Query Type	Policy	Message	Domain Filter List	Category	Category Description
2019/04/05 11:06:48	dns	10.1.100.18	cpe-98-25-53-166.sc.res.rr.com	A	1	Domain was blocked by dns botnet C&C			
2019/04/05 11:06:48	dns	10.1.100.18	cpe-98-25-53-166.sc.res.rr.com	A	1				

### To check the DNS Filter log in the CLI:

```
1: date=2019-04-05 time=11:06:48 logid="1501054600" type="utm" subtype="dns" eventtype="dns-
response" level="warning" vd="vdom1" eventtime=1554487606 policyid=1 sessionid=55232
srcip=10.1.100.18 srcport=60510 srcintf="port10" srcintfrole="undefined" dstip=172.16.95.16
dstport=53 dstintf="port9" dstintfrole="undefined" proto=17 profile="demo" xid=16265
qname="cpe-98-25-53-166.sc.res.rr.com" qtype="A" qtypeval=1 qclass="IN"
ipaddr="93.184.216.34" msg="Domain was blocked by dns botnet C&C" action="redirect"
botnetip=98.25.53.166
```

```
2: date=2019-04-05 time=11:06:48 logid="1500054000" type="utm" subtype="dns" eventtype="dns-
query" level="information" vd="vdom1" eventtime=1554487606 policyid=1 sessionid=55232
srcip=10.1.100.18 srcport=60510 srcintf="port10" srcintfrole="undefined" dstip=172.16.95.16
dstport=53 dstintf="port9" dstintfrole="undefined" proto=17 profile="demo" xid=16265
qname="cpe-98-25-53-166.sc.res.rr.com" qtype="A" qtypeval=1 qclass="IN"
```

### To check botnet activity:

1. Go to **Dashboard > Status** and see the **Botnet Activity** widget.

If you cannot find the **Botnet Activity** widget, click the **Settings** button at the bottom right, select **Add Widget**, and add the **Botnet Activity** widget.

Botnet Activity	
Known IPs	13586
Known Domains	55583
Activity Since	2019/04/04 11:51:03
Blocked IPs	0
Blocked Domains	1
Blocked Connections	3

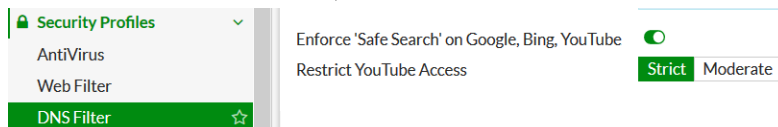
## DNS safe search

Enable DNS Filter safe search so that FortiGate responds with the search engine's children and school safe domain or IP address. Users might not be aware of this filter. Explicit contents are filtered by the search engine itself. This feature isn't 100% accurate but it can help you avoid explicit and inappropriate search results.

This feature currently supports Google, Bing, and YouTube.

### To configure DNS Filter Safe Search on GUI:

1. Go to *Security Profiles > DNS Filter* and edit or create a DNS Filter.
2. Enable *Enforce 'Safe search' on Google, Bing, YouTube*.
3. For *Restrict YouTube Access*, select *Strict* or *Moderate*.



### To configure DNS Filter Safe Search on CLI:

```
config dnsfilter profile
 edit "demo"
 config ftgd-dns
 set options error-allow
 config filters
 edit 2
 set category 2
 next
 ...
 end
 end
 set log-all-domain enable
 set block-botnet enable
 set safe-search enable <<<==== DNS Filter Safe Search option
next
end
```

### Sample

To see an example of how this works, enable this option. Then from your internal network PC, use a command line tool such as `dig` or `nslookup` to do a DNS query on `www.bing.com`. For example:

```
dig www.bing.com
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 46568
;; Flags: qr rd ra; QUERY: 1; ANSWER: 2; AUTHORITY: 0; ADDITIONAL: 0

;; QUESTION SECTION:
;; www.bing.com. IN A

;; ANSWER SECTION:
www.bing.com. 103 IN CNAME strict.bing.com. <<<====
strict.bing.com. 103 IN A 204.79.197.220

;; Received 67 B
;; Time 2019-04-05 14:34:52 PDT
;; From 172.16.95.16@53 (UDP) in 196.0 ms
```

The DNS query for `www.bing.com` returns with a CNAME `strict.bing.com`, and A record for the CNAME. The user's web browser then connects to this address with the same search engine UI but any explicit content search is filtered out. Check the DNS Filter log for the message *DNS Safe Search enforced*.

Date/Time	Sub Type	Source	Domain Name	Query Type	Policy	Message	Domain Filter List	Category	Category Description
2019/04/05 14:34:53	dns	10.1.100.18	www.bing.com	A	1	DNS Safe Search enforced		41	Search Engines and Portals
2019/04/05 14:34:53	dns	10.1.100.18	www.bing.com	A	1				



**To check the DNS Filter Safe Search log in the CLI:**

```
1: date=2019-04-05 time=14:34:53 logid="1501054804" type="utm" subtype="dns" eventtype="dns-
response" level="notice" vd="vdom1" eventtime=1554500093 policyid=1 sessionid=65955
srcip=10.1.100.18 srcport=36575 srcintf="port10" srcintfrole="undefined" dstip=172.16.95.16
dstport=53 dstintf="port9" dstintfrole="undefined" proto=17 profile="demo" xid=59573
qname="www.bing.com" qtype="A" qtypeval=1 qclass="IN" ipaddr="204.79.197.220" msg="DNS Safe
Search enforced" action="pass" sscname="strict.bing.com" cat=41 catdesc="Search Engines and
Portals"
```

```
2: date=2019-04-05 time=14:34:53 logid="1500054000" type="utm" subtype="dns" eventtype="dns-
query" level="information" vd="vdom1" eventtime=1554500092 policyid=1 sessionid=65955
srcip=10.1.100.18 srcport=36575 srcintf="port10" srcintfrole="undefined" dstip=172.16.95.16
dstport=53 dstintf="port9" dstintfrole="undefined" proto=17 profile="demo" xid=59573
qname="www.bing.com" qtype="A" qtypeval=1 qclass="IN"
```

**Additional information**

For each search engine's safe search specifications, see its specification page:

- <https://help.bing.microsoft.com/#apex/18/en-US/10003/0>
- <https://support.google.com/websearch/answer/510?co=GENIE.Platform%3DDesktop&hl=en>
- <https://support.google.com/youtube/answer/174084?co=GENIE.Platform%3DDesktop&hl=en>

**Local domain filter**

In addition to FortiGuard's category-based domain filter, you can also can define your own local static domain filter to allow or block specific domains.

**To configure DNS local domain filter on GUI:**

1. Go to *Security Profiles > DNS Filter* and edit or create a DNS Filter.
2. In the *Static Domain Filter* section, enable *Domain Filter*.
3. Click *Create New* to create your local domain filter entries.

Static Domain Filter

Domain Filter ☒

Domain	Type	Action	Status
www.fortinet.com	simple	Allow	Enable
*example.com	wildcard	Redirect to Block Portal	Enable
google	regex	Monitor	Enable

3

**To configure DNS local domain filter on CLI:**

```
config dnsfilter domain-filter
edit 1
set name "demo"
set comment ''
config entries
edit 1
```

```

 set domain "www.fortinet.com"
 set type simple
 set action allow
 set status enable
 next
 edit 2
 set domain "*.example.com"
 set type wildcard
 set action block
 set status enable
 next
 edit 3
 set domain "google"
 set type regex
 set action monitor
 set status enable
 next
end
next
end

```

Wildcard entries are converted to regular expressions by FortiOS. As a result of this conversion, wildcards will match any suffix, as long as there is a word boundary following the search term.

For example:

```

config entries
 edit 1
 set domain "*.host"
 set type wildcard
 next
end

```



will match `wp36.host` and `wp36.host.pressdns.com`, but not `wp36.host123.pressdns.com`.

To avoid this, use an explicit regular expression search string:

```

config entries
 edit 1
 set domain "^.*\\.host$"
 set type regexp
 next
end

```

## To check the DNS local domain filter log in the GUI:

1. Go to **Log & Report > DNS Query** to view the DNS query log.

Date/Time	Sub Type	Source	Domain Name	Query Type	Policy	Message	Domain Filter List	Category	Category Description
2019/04/05 15:37:06	dns	10.1.100.18	www.google.com	A	1	Domain belongs to a denied category in policy		41	Search Engines and Port
2019/04/05 15:37:06	dns	10.1.100.18	www.google.com	A	1				
2019/04/05 15:36:59	dns	10.1.100.18	www.example.com	A	1	Domain was blocked because it is in the domain-filter list	demo		
2019/04/05 15:36:59	dns	10.1.100.18	www.example.com	A	1				
2019/04/05 15:36:51	dns	10.1.100.18	www.fortinet.com	A	1	Domain was allowed because it is in the domain-filter list	demo		
2019/04/05 15:36:51	dns	10.1.100.18	www.fortinet.com	A	1				

Since the local domain list "google" action is Monitor, it's blocked by FortiGuard category-based domain filter.

### To check the DNS local domain filter log in the CLI:

```
7: date=2019-04-05 time=15:37:06 logid="1501054803" type="utm" subtype="dns" eventtype="dns-response" level="warning" vd="vdom1" eventtime=1554503826 policyid=1 sessionid=69132 srcip=10.1.100.18 srcport=49832 srcintf="port10" srcintfrole="undefined" dstip=172.16.95.16 dstport=53 dstintf="port9" dstintfrole="undefined" proto=17 profile="demo" xid=4612 qname="www.google.com" qtype="A" qtypeval=1 qclass="IN" ipaddr="208.91.112.55" msg="Domain belongs to a denied category in policy" action="redirect" cat=41 catdesc="Search Engines and Portals"
```

```
8: date=2019-04-05 time=15:37:06 logid="1500054000" type="utm" subtype="dns" eventtype="dns-query" level="information" vd="vdom1" eventtime=1554503826 policyid=1 sessionid=69132 srcip=10.1.100.18 srcport=49832 srcintf="port10" srcintfrole="undefined" dstip=172.16.95.16 dstport=53 dstintf="port9" dstintfrole="undefined" proto=17 profile="demo" xid=4612 qname="www.google.com" qtype="A" qtypeval=1 qclass="IN"
```

```
9: date=2019-04-05 time=15:36:59 logid="1501054400" type="utm" subtype="dns" eventtype="dns-response" level="warning" vd="vdom1" eventtime=1554503818 policyid=1 sessionid=69121 srcip=10.1.100.18 srcport=40659 srcintf="port10" srcintfrole="undefined" dstip=172.16.95.16 dstport=53 dstintf="port9" dstintfrole="undefined" proto=17 profile="demo" xid=24730 qname="www.example.com" qtype="A" qtypeval=1 qclass="IN" msg="Domain was blocked because it is in the domain-filter list" action="redirect" domainfilteridx=1 domainfilterlist="demo"
```

```
10: date=2019-04-05 time=15:36:59 logid="1500054000" type="utm" subtype="dns" eventtype="dns-query" level="information" vd="vdom1" eventtime=1554503818 policyid=1 sessionid=69121 srcip=10.1.100.18 srcport=40659 srcintf="port10" srcintfrole="undefined" dstip=172.16.95.16 dstport=53 dstintf="port9" dstintfrole="undefined" proto=17 profile="demo" xid=24730 qname="www.example.com" qtype="A" qtypeval=1 qclass="IN"
```

```
11: date=2019-04-05 time=15:36:51 logid="1501054401" type="utm" subtype="dns" eventtype="dns-response" level="information" vd="vdom1" eventtime=1554503810 policyid=1 sessionid=69118 srcip=10.1.100.18 srcport=33461 srcintf="port10" srcintfrole="undefined" dstip=172.16.95.16 dstport=53 dstintf="port9" dstintfrole="undefined" proto=17 profile="demo" xid=53801 qname="www.fortinet.com" qtype="A" qtypeval=1 qclass="IN" ipaddr="13.56.55.78, 54.183.57.55" msg="Domain was allowed because it is in the domain-filter list" action="pass" domainfilteridx=1 domainfilterlist="demo"
```

```
12: date=2019-04-05 time=15:36:51 logid="1500054000" type="utm" subtype="dns" eventtype="dns-query" level="information" vd="vdom1" eventtime=1554503810 policyid=1 sessionid=69118 srcip=10.1.100.18 srcport=33461 srcintf="port10" srcintfrole="undefined" dstip=172.16.95.16 dstport=53 dstintf="port9" dstintfrole="undefined" proto=17 profile="demo" xid=53801 qname="www.fortinet.com" qtype="A" qtypeval=1 qclass="IN"
```

## Sequence and priority

In DNS Filter, local domain filter has a higher priority than FortiGuard category-based domain filter.

A DNS query is scanned and matched with local domain filter first. If an entry matches and the local filter entry's action is block, then that DNS query is blocked or redirected.

If local domain filter list has no match, then the FortiGuard category-based domain filter is used. If a DNS query domain name rating belongs to the block category, this query is blocked or redirected. If the FortiGuard category-based filter has no match, then the original resolved IP address is returned to the client DNS resolver.

The local domain filter action can be Block, Allow, or Monitor. If the local domain filter action is Allow and an entry matches, it will skip the FortiGuard category-based domain filter and directly return to client DNS resolver. If the local domain filter action is Monitor and an entry matches, it will go to FortiGuard category-based domain filter scanning and matching.

## DNS translation

Using this feature, you can translate a DNS resolved IP address to another IP address you specify on a per-policy basis.

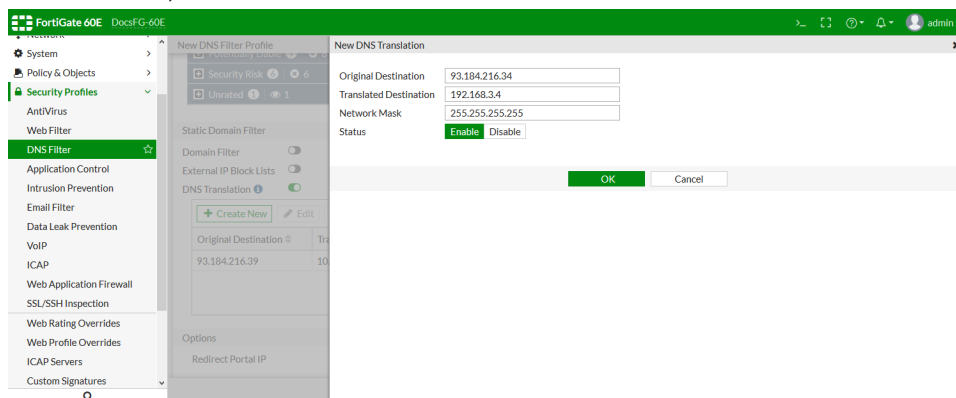
For example, website A has a public address 1.2.3.4. However, when your internal network users visit this website, you want them to connect to an internal host, say, 192.168.3.4. In this case, you can use DNS translation to translate the DNS resolved address 1.2.3.4 to 192.168.3.4. Reverse use of DNS translation is also applicable, for example, if you want public DNS query of your internal server to get a public IP address, then you can translate a DNS resolved private IP to a public IP address.

### Example

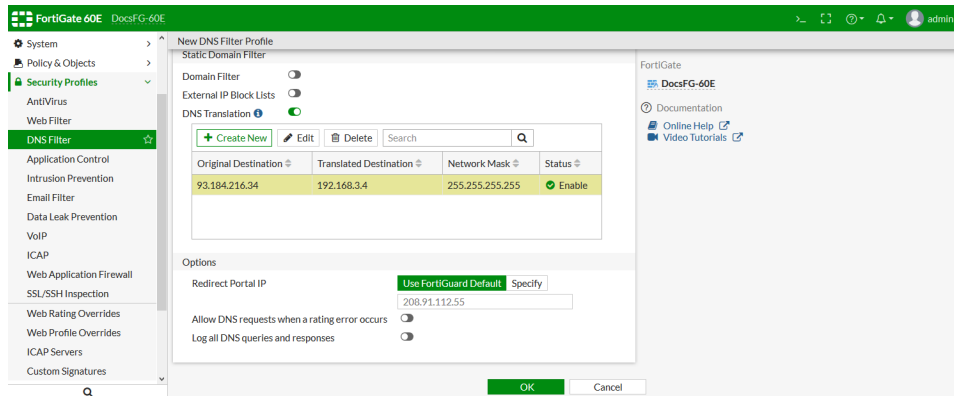
This example configuration forces the DNS Filter profile to translate 93.184.216.34 (www.example.com) to 192.168.3.4. When internal network users do a DNS query for www.example.com, they do not get the original www.example.com IP address of 93.184.216.34. Instead, it is replaced with 192.168.3.4.

#### To configure DNS translation in the GUI:

1. Go to *Security Profiles > DNS Filter* and edit or create a DNS Filter profile.
2. Enable *DNS Translation* and click *Create New*.
3. Enter the *Original Destination* (the domain's original IP address), the *Translated Destination* IP address, and the *Network Mask*, and set *Status* to *Enable*.



## 4. Click OK.



## 5. Click OK to create or edit the DNS profile.

**To configure DNS translation in the CLI:**

```
config dnsfilter profile
 edit "demo"
 set comment ''
 ...
 config dns-translation
 edit 1
 set src 93.184.216.34
 set dst 192.168.3.4
 set netmask 255.255.255.255
 next
 end
 set redirect-portal 0.0.0.0
 set redirect-portal6 ::
 set youtube-restrict strict
 next
end
```

**To check DNS translation using a command line tool before DNS translation:**

```
dig www.example.com
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 27030
;; Flags: qr rd ra; QUERY: 1; ANSWER: 1; AUTHORITY: 2; ADDITIONAL: 0

;; QUESTION SECTION:
;; www.example.com. IN A

;; ANSWER SECTION:
www.example.com. 33946 IN A 93.184.216.34

;; AUTHORITY SECTION:
example.com. 18578 IN NS b.iana-servers.net.
example.com. 18578 IN NS a.iana-servers.net.

;; Received 97 B
;; Time 2019-04-08 10:47:26 PDT
;; From 172.16.95.16@53(UDP) in 0.5 ms
```

**To check DNS translation using a command line tool after DNS translation:**

```
dig www.example.com
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 62060
;; Flags: qr rd ra; QUERY: 1; ANSWER: 1; AUTHORITY: 2; ADDITIONAL: 0

;; QUESTION SECTION:
;; www.example.com. IN A

;; ANSWER SECTION:
www.example.com. 32491 IN A 192.168.3.4 <<<==== resolved IP translated
into 192.168.3.4

;; AUTHORITY SECTION:
example.com. 17123 IN NS b.iana-servers.net.
example.com. 17123 IN NS a.iana-servers.net.

;; Received 97 B
;; Time 2019-04-08 11:11:41 PDT
;; From 172.16.95.16@53(UDP) in 0.5 ms
```

**DNS translation network mask**

The following is an example of DNS translation and result:

```
config dns-translation
 edit 1
 set src 93.184.216.34
 set dst 1.2.3.4
 set netmask 255.255.224.0
 next
end

dig www.example.com
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 6736
;; Flags: qr rd ra; QUERY: 1; ANSWER: 1; AUTHORITY: 2; ADDITIONAL: 0

;; QUESTION SECTION:
;; www.example.com. IN A

;; ANSWER SECTION:
www.example.com. 29322 IN A 1.2.24.34

;; AUTHORITY SECTION:
example.com. 13954 IN NS a.iana-servers.net.
example.com. 13954 IN NS b.iana-servers.net.

;; Received 97 B
;; Time 2019-04-08 12:04:30 PDT
;; From 172.16.95.16@53(UDP) in 2.0 ms

1) AND src(Original IP) with negative netmask (93.184.216.34 & ~255.255.224.0)
01011101.10111000.11011000.00100010 93.184.216.34 <-- ip
00000000.00000000.00011111.11111111 ~255.255.224.0 <-- ~netmask
----- &
00000000.00000000.00011000.00100010 0.0.24.34 <- right bits
```

```

2) AND dst(Translated IP) with netmask
00000001.00000010.00000011.00000100 1.2.3.4 <- dst
11111111.11111111.11100000.00000000 255.255.224.0 <- netmask
----- &
00000001.00000010.00000000.00000000 1.2.0.0 <- left bits

3) Final step 2 bitwise-OR 3:
00000000.00000000.00011000.00100010 0.0.24.34
00000001.00000010.00000000.00000000 1.2.0.0
----- |
00000001.00000010.00011000.00100010 1.2.24.34

```

## Using a FortiGate as a DNS server

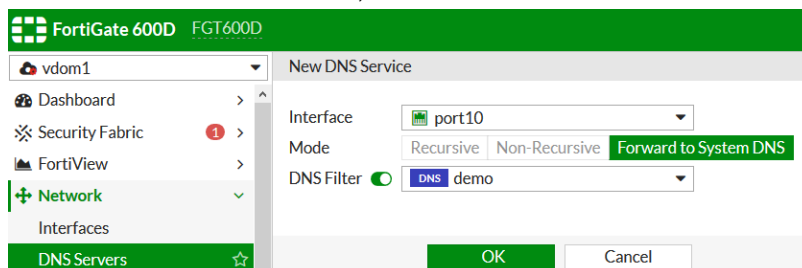
You can configure and use FortiGate as a DNS server in your network. When you enable DNS Service on a specific interface, FortiGate will listen for DNS Service on that interface.

Depending on the configuration, DNS Service on FortiGate can work in three modes: *Recursive*, *Non-Recursive*, or *Forward to System DNS* (server). For details on how to configure DNS Service on FortiGate, see the FortiGate System Configuration Guide.

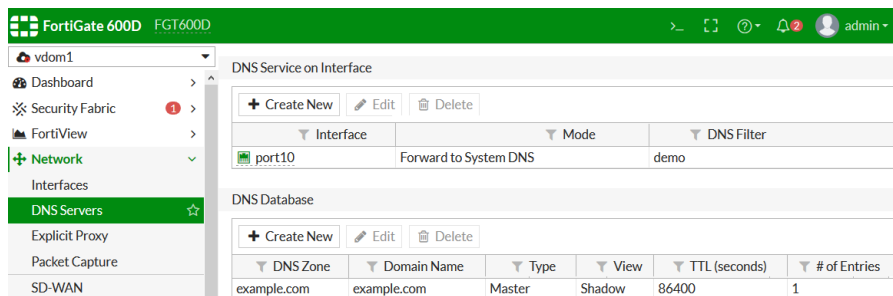
You can apply a DNS Filter profile to Recursive Mode and Forward to System DNS Mode. This is the same as FortiGate working as a transparent DNS Proxy for DNS relay traffic.

### To configure DNS Service on FortiGate using GUI:

1. Go to *Network > DNS Servers*.
2. In the *DNS Service on Interface*, click *Create New* and select an *Interface*.



The *Recursive* and *Non-Recursive* Mode is available only after you configure the DNS database.



**To configure DNS Service on FortiGate using CLI:**

```
config system dns-server
 edit "port10" <<<==== Enable DNS Service on Interface
 set mode forward-only
 set dnsfilter-profile "demo" <<<==== apply DNS Filter Profile for the service
 next
end
```

**Sample configuration**

In this example, FortiGate port 10 is enabled as a DNS Service with the DNS Filter profile "demo". Suppose port 10 has an IP address 10.1.100.5 and DNS Filter profile "demo" is set to block category 52 (Information Technology), then from your internal network PC, use a command line tool such as dig or nslookup to do a DNS query. For example:

```
dig @10.1.100.5 www.fortinet.com <<<====Specify FortiGate interface address as DNS
Server
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 52809
;; Flags: qr rd; QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 0

;; QUESTION SECTION:
;; www.fortinet.com. IN A

;; ANSWER SECTION:
www.fortinet.com. 60 IN A 208.91.112.55 <<<==== DNS Filter profile
will filter the relay DNS traffic based on profile configuration. It blocked with redirect
portal IP

;; Received 50 B
;; Time 2019-04-08 14:36:34 PDT
;; From 10.1.100.5@53(UDP) in 13.6 ms
```

**Troubleshooting for DNS filter**

If you have trouble with the DNS Filter profile in your policy, start with the following troubleshooting steps:

- [Check the connection between FortiGate and FortiGuard DNS rating server \(SDNS server\).](#)
- [Check that FortiGate has a valid FortiGuard Web Filter license.](#)
- [Check the FortiGate DNS Filter configuration.](#)

**Troubleshooting connection between FortiGate and FortiGuard SDNS server**

Ensure FortiGate can connect to the FortiGuard SDNS server. By default, FortiGate uses UDP port 53 to connect to the SDNS server.

**To check the connection between FortiGate and the SDNS server in the CLI:**

1. In the CLI Console, run the command `diagnose test application dnsproxy 3` to find the FortiGuard SDNS server.

```
worker idx: 0
vdom: root, index=0, is master, vdom dns is disabled, mip-169.254.0.1 dns_log=1
```



```

dns64 is disabled
vdom: vdom1, index=1, is master, vdom dns is enabled, mip-169.254.0.1 dns_log=1
dns64 is disabled
dns-server:208.91.112.220:53 tz=-480 req=0 to=0 res=0 rt=0 secure=1 ready=1 timer=0
probe=0 failure=0 last_failed=0
dns-server:208.91.112.53:53 tz=0 req=0 to=0 res=0 rt=0 secure=0 ready=1 timer=0 probe=0
failure=0 last_failed=0
dns-server:208.91.112.52:53 tz=0 req=0 to=0 res=0 rt=0 secure=0 ready=1 timer=0 probe=0
failure=0 last_failed=0
dns-server:62.209.40.75:53 tz=60 req=0 to=0 res=0 rt=0 secure=1 ready=1 timer=0 probe=0
failure=0 last_failed=0
dns-server:209.222.147.38:53 tz=-300 req=0 to=0 res=0 rt=0 secure=1 ready=1 timer=0
probe=0 failure=0 last_failed=0
dns-server:173.243.138.221:53 tz=-480 req=0 to=0 res=0 rt=0 secure=1 ready=1 timer=0
probe=0 failure=0 last_failed=0
dns-server:45.75.200.89:53 tz=0 req=0 to=0 res=0 rt=0 secure=1 ready=1 timer=0 probe=0
failure=0 last_failed=0
DNS_CACHE: hash-size=2048, ttl=1800, min-ttl=60, max-num=5000
DNS_FD: udp_s=13 udp_c=16:17 ha_c=21 unix_s=22, unix_nb_s=23, unix_nc_s=24
 v6_udp_s=12, v6_udp_c=19:20, snmp=25, redir=14
DNS_FD: tcp_s=27, tcp_s6=26, redir=28
FQDN: hash_size=1024, current_query=1024
DNS_DB: response_buf_sz=4096
LICENSE: expiry=2029-08-21, expired=0, type=2
FDG_SERVER:208.91.112.220:53
FGD_CATEGORY_VERSION:8
SERVER_LDB: gid=6f00, tz=-420, error_allow=0
FGD_REDIR:208.91.112.55

```

2. Check the **FDG\_SERVER** line. The SDNS server IP address might be different depending on location. For this example, it is:

```
FDG_SERVER:208.91.112.220:53
```

3. In the CLI Console under the management VDOM, run the command `execute ping 208.91.112.220` to check the communication between the FortiGate and the SDNS server.
4. Optionally, you can also check the communication using a PC on the internal network.
  - a. Disable the DNS Filter profile so that it does not affect your connection check.
  - b. Ping your ISP or a public DNS service provides's DNS server, for example, Google's public DNS server of 8.8.8.8:

```
#dig @8.8.8.8 www.fortinet.com
```

Or specify the SDNS server as DNS server:

```
#dig @208.91.112.220 www.fortinet.com
```

- c. Check that you can get domain `www.fortinet.com` A record from the DNS server which shows that UDP port 53 connection path is not blocked.

```

#dig @8.8.8.8 www.fortinet.com
;; ->>HEADER<<- opcode: QUERY; status: NOERROR; id: 35121
;; Flags: qr rd ra; QUERY: 1; ANSWER: 3; AUTHORITY: 0; ADDITIONAL: 0

;; QUESTION SECTION:
;; www.fortinet.com. IN A

```

```
;; ANSWER SECTION:
www.fortinet.com. 289 IN CNAME fortinet-prod4-858839915.us-west-
1.elb.amazonaws.com.
fortinet-prod4-858839915.us-west-1.elb.amazonaws.com. 51 IN A
52.8.142.247
fortinet-prod4-858839915.us-west-1.elb.amazonaws.com. 51 IN A
13.56.55.78

;; Received 129 B
;; Time 2019-04-29 14:13:18 PDT
;; From 8.8.8.8@53 (UDP) in 13.2 ms
```

## Checking FortiGuard DNS Rating Service license

The FortiGuard DNS Rating Service shares the license with FortiGuard Web Filter so you must have a valid Web Filter license for the DNS Rating Service to work. While the license is shared, the DNS Rating Service uses a separate connection mechanism from the Web Filter Rating.

### To check the DNS Rating Service license in the CLI:

1. In the CLI Console, run the command `diagnose test application dnsproxy 3`.
2. Look for the `LICENSE` line and check that the license has not expired, for example:

```
LICENSE: expiry=2029-08-21, expired=0, type=2
```

3. Check the `sdns-server` lines to show the functioning servers:

```
sdns-server:208.91.112.220:53 tz=-480 tls=0 req=0 to=0 res=0 rt=4 ready=1 timer=0
probe=0 failure=0 last_failed=0
```

## Checking FortiGate DNS Filter profile configuration

### To check the FortiGate DNS Filter profile configuration:

1. Create a local domain filter and set the *Action to Redirect to Block Portal*.  
See [Local domain filter on page 1011](#).
2. Apply this DNS Filter profile to the policy.
3. From the client PC, DNS query this domain.

If you get the profile's redirected portal address, that shows that the DNS Filter profile works as expected.

## More troubleshooting steps

### To reload the DNS proxy in the CLI:

```
(global)#diagnose test application dnsproxy 99
```

### To debug DNS proxy details:

These commands might create more output in your console.

```
#diagnose debug application dnsproxy -1
```

```
#diagnose debug enable/disable
```

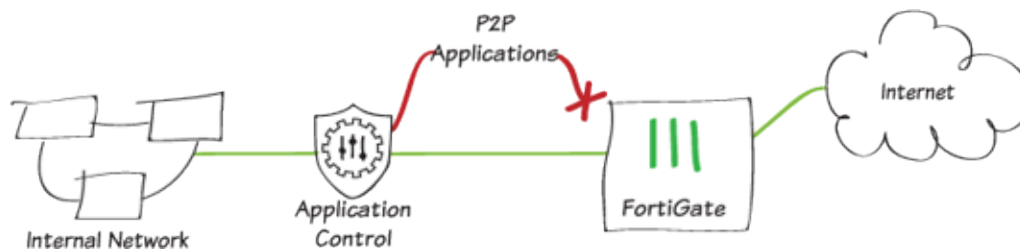
## DNS proxy command reference

Use `diagnose test application dnsproxy <test level>` to troubleshoot further DNS proxy information, where:

Test level	Action
1	Clear DNS cache
2	Show statistics
3	Dump DNS setting
4	Reload FQDN
5	Requery FQDN
6	Dump FQDN
7	Dump DNS cache
8	Dump DNS database
9	Reload DNS database
10	Dump secure DNS policy/profile
11	Dump botnet domain
12	Reload secure DNS setting
13	Show hostname cache
14	Clear hostname cache
15	Show SDNS rating cache
16	Clear SDNS rating cache
17	Show DNS debug bit mask
99	Restart the dnsproxy worker

## Application control

FortiGates can recognize network traffic generated by a large number of applications. Application control sensors specify what action to take with the application traffic. Application control uses IPS protocol decoders that can analyze network traffic to detect application traffic, even if the traffic uses non-standard ports or protocols. Application control supports traffic detection using the HTTP protocol (versions 1.0, 1.1, and 2.0).



FortiOS includes three preloaded application sensors:

- *default* (monitors all applications)
- *wifi-default* (default configuration for offloading WiFi traffic)
- *block-high-risk*

You can customize these sensors, or you can create your own to log and manage the applications on your network.

Once configured, you can add the application sensor to a firewall policy.



This functionality requires a subscription to FortiGuard Application Control.

The following topics provide information about application control:

- [Basic category filters and overrides on page 1022](#)
- [Port enforcement check on page 1026](#)
- [Protocol enforcement on page 1027](#)

## Basic category filters and overrides

Once you have created an application sensor, you can define the applications that you want to control. You can add applications and filters using categories, application overrides, and/or filter overrides.

- **Categories:** Choose groups of signatures based on a category type.
- **Application overrides:** Choose individual applications.
- **Filter overrides:** Select groups of applications and override the application signature settings for them.

### Categories

Categories allow you to choose groups of signatures based on a category type. Applications belonging to the category trigger the action that is set for the category.

#### To set category filters in the CLI:

```
config application list
 edit {id}
 config entries
 edit 1
 set category <id>
 ID Select Category ID
 2 P2P
```

```

3 VoIP
5 Video/Audio
6 Proxy
7 Remote.Access
8 Game
12 General.Interest
15 Network.Service
17 Update
21 Email
22 Storage.Backup
23 Social.Media
25 Web.Client
26 Industrial
28 Collaboration
29 Business
30 Cloud.IT
31 Mobile
 set action {pass | block | reset}
 pass Pass or allow matching traffic.
 block Block or drop matching traffic.
 reset Reset sessions for matching traffic.
 set log {enable | disable}
next
end
next
end
```

### To set category filters in the GUI:

1. Go to *Security Profiles > Application Control*.
2. Under *Categories*, left click the icon next to the category name to view a dropdown of actions:
  - Allow
  - Monitor
  - Block
  - Quarantine
  - View signatures
3. Select *OK*.

Categories

▼ All Categories

▼ Business (140, ☁ 6)

▼ Email (78, ☁ 12)

▼ Mobile (3)

▼ Proxy (165)

▼ Storage.Backup (162, ☁ 17)

▼ VoIP (24)

▼ Cloud.IT (45)

▼ Game (84)

▼ Network.Service (329)

▼ Remote.Access (82)

▼ Update (49)

▼ Web.Client (23)

▼ Monitor

✓ Allow

✗ Block

🚫 Quarantine

📋 View Signatures (23)

▼ Collaboration (252, ☁ 10)

▼ General.Interest (224, ☁ 7)

▼ P2P (59)

▼ Social.Media (118, ☁ 31)

▼ Video/Audio (150, ☁ 14)

✓ Unknown Applications

☐ Network Protocol Enforcement

Application and Filter Overrides

+ Create New

✎ Edit

🗑 Delete

## Application and filter overrides

Override type	Setting
<b>Application</b>	<p><b>Type:</b> Choose <i>Application</i> for application overrides.</p> <p><b>Action:</b> Can be set to Monitor/Allow/Block/Quarantine.</p> <p><b>Application:</b> Multiple app signatures can be added for one entry. A slide-in presenting an application list will be shown to select specific app signatures, and the search box can be used to filter matched signatures.</p>
<b>Filter</b>	<p><b>Type:</b> Choose <i>Filter</i> for filter overrides.</p> <p><b>Action:</b> Can be set to Monitor/Allow/Block/Quarantine.</p> <p><b>Filter:</b> Filters can be selected by behavior, application category, technology, popularity, protocol, risk, or vendor subtypes.</p> <p><b>Search box:</b> Can be used to determine if the input signature is included in selected filters, where matched applications are shown at the bottom.</p>

### To set overrides in the CLI:

```

config application list
 edit {id}
 config entries
 edit 1
 set protocols <0-47> #network protocol ID
 set risk <id>
 *level Risk of allowing traffic from this application to occur (1 -
5; Low, Elevated, Medium, High, and Critical).
 set vendor <0-25> #vendor ID
 set technology <id>
 All All
 0 Network-Protocol

```

FortiOS 6.2.15 Cookbook  
Fortinet Inc.

1024

```

1 Browser-Based
2 Client-Server
4 Peer-to-Peer

set behavior <id>
All All
2 Botnet
3 Evasive
5 Excessive-Bandwidth
6 Tunneling
9 Cloud

set popularity <1-5> #Popularity level 1-5
set action {pass | block | reset}
pass Pass or allow matching traffic.
block Block or drop matching traffic.
reset Reset sessions for matching traffic.

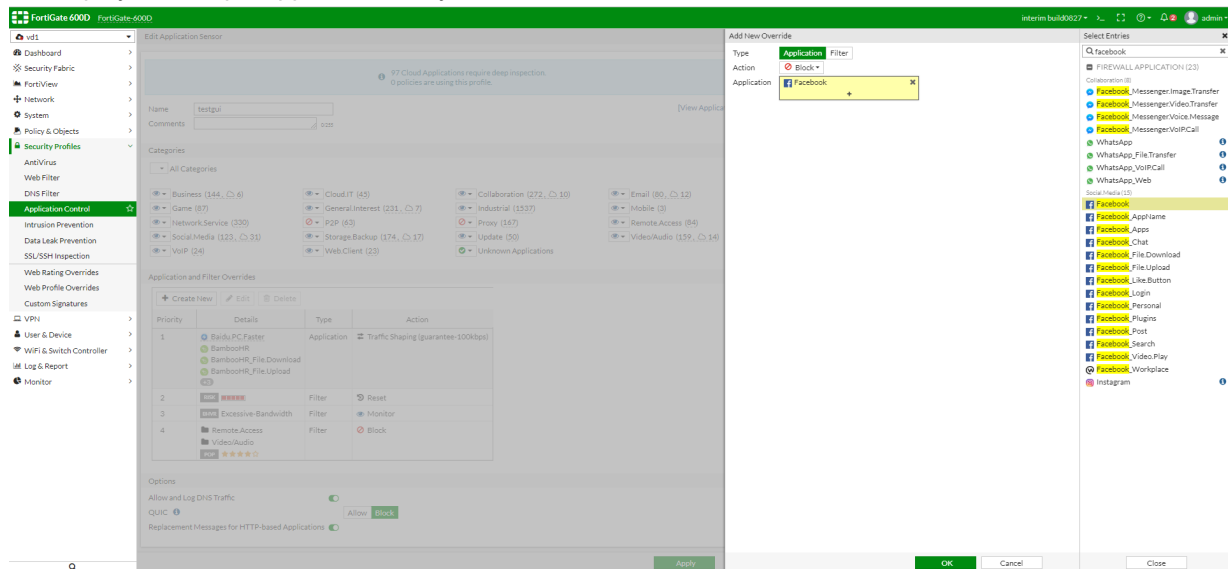
set log {enable | disable}

next
end
next
end

```

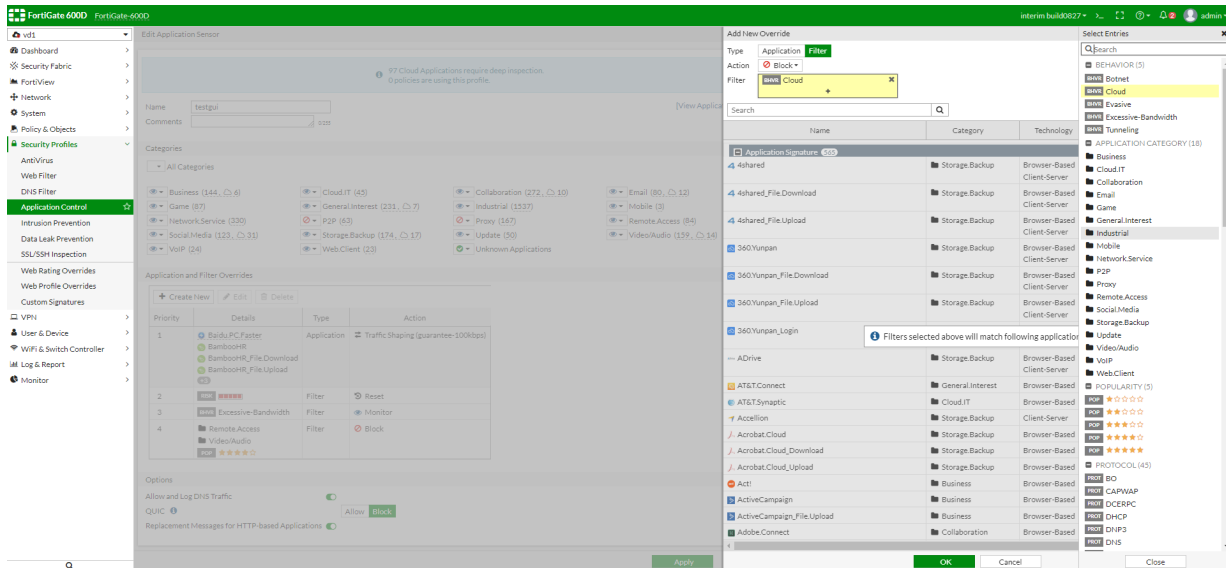
### To set overrides in the GUI:

1. Go to *Security Profiles > Application Control*.
2. Under the *Application and Filter Overrides* table, click *Create New*.
3. To add individual applications:
  - a. Select *Application* as the *Type*.
  - b. Choose an action to be associated with the application.
  - c. Click the + button in the *Application* field and choose the specific applications from the list where app signatures are displayed. Multiple applications may be selected.



- d. Click *OK*.
4. To add advanced filters:
    - a. Create another entry in the *Application and Filter Overrides* table.
    - b. Select *Filter* as the *Type*.

- c. Select *Cloud* under the behavior section from the *Select Entries* list. Matched signatures are shown along the bottom.



- d. Click OK.

## Port enforcement check

Most networking applications run on specific ports. For example, SSH runs on port 22, and Facebook runs on ports 80 and 443.

If the default network service is enabled in the Application Control profile, a port enforcement check is done at the application profile level, and any detected application signatures running on the non-standard TCP/IP port are blocked. This means that each application allowed by the app control sensor is only run on its default port.

### To set port enforcement check in the CLI:

```
config application list
 edit "default_port"
 set enforce-default-app-port {enable | disable}
 disable Disable default application port enforcement.
 enable Enable default application port enforcement.
 config entries
 edit 1
 set application 15896
 set action pass
 next
 end
next
end
```

For example, when applying the above appctrl sensor, FTP traffic with the standard port (port 21) is allowed, while the non-standard port (port 2121) is blocked.



## Protocol enforcement

Protocol enforcement allows you to configure networking services (e.g. FTP, HTTP, HTTPS) on known ports (e.g. 21, 80, 443). For protocols that are not allowlisted under select ports, the IPS engine performs the violation action to block, allow, or monitor that traffic.

This feature can be used in the following scenarios::

- When one protocol dissector confirms the service of network traffic, protocol enforcement can check whether the confirmed service is allowlisted under the server port. If it is not Allowlisted, the traffic is considered a violation and IPS can take the action specified in the configuration (block or monitor it).
- When there is no confirmed service for the network traffic, the traffic is considered a service violation if IPS dissectors rule out all of the services enforced under its server port.

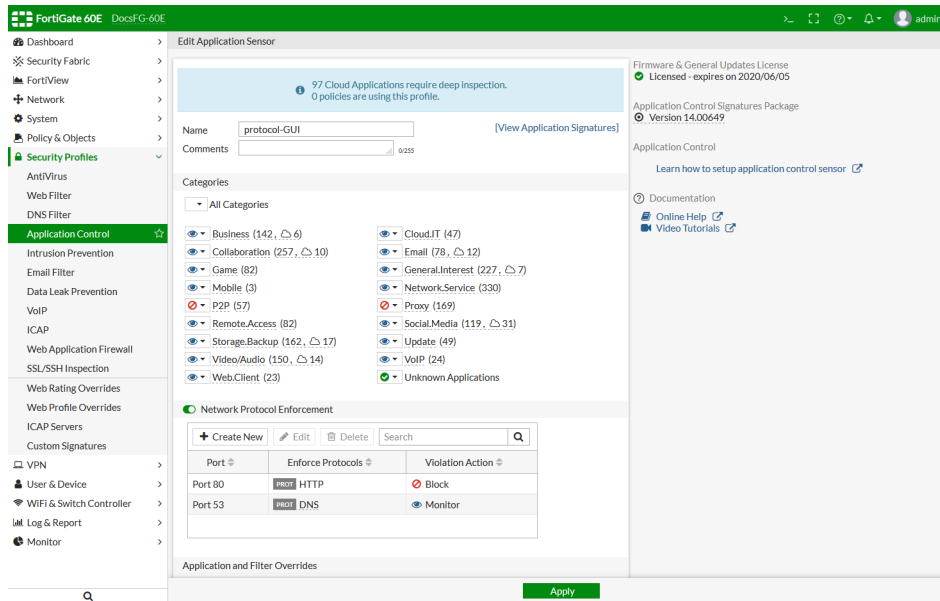
In an applicable profile, a default-network-service list can be created to associate well known ports with accepted services.

### To setup protocol enforcement in the CLI:

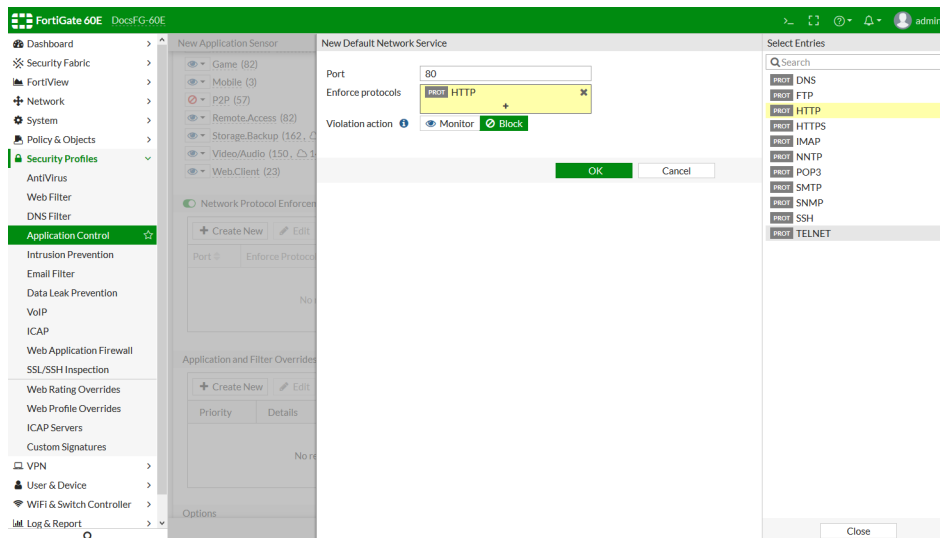
```
config application list
 edit "protocol-GUI"
 set other-application-log enable
 set control-default-network-services {enable | disable} # Enable/Disable enforcement
of protocols over select ports
 config default-network-services # Default network service
entries
 edit 1
 set port 80 # Port number, enter an integer value from <0>
to <65535>
 set services http # Network protocols: http, ssh, ftp, dns,
smtp, pop3, imap, snmp, nntp, and https
 next
 edit 2
 set port 53
 set services dns
 set violation-action {pass | monitor | block} # Pass, Log, or block when
non-DNS traffic run over port 53
 next
 end
next
end
```

### To setup protocol enforcement in the GUI:

1. Go to *Security Profiles > Application Control*.
2. Create a new application sensor or edit an existing one.
3. Enable *Network Protocol Enforcement*.  
Enforcement entries can be created, edited, or deleted to configure network services on certain ports and determine the violation action.



4. Click **Create New** in the **Network Protocol Enforcement** table.



5. In the **New Default Network Service** pane:

- Enter a *Port* number.
- Select *Enforced protocols*.
- Choose the *Violation action*.
- Click **OK**.

6. Click **OK**.

## Intrusion prevention

Intrusion Prevention System (IPS) detects network attacks and prevents threats from compromising the network, including protected devices. IPS can be in the form of a standalone appliance, or part of the feature set of a Next

Generation Firewall (NGFW), such as FortiGate. IPS utilizes signatures, protocol decoders, heuristics (or behavioral monitoring), threat intelligence (such as FortiGuard Labs), and advanced threat detection in order to prevent exploitation of known and unknown zero-day threats. FortiGate IPS is even capable of performing deep packet inspection to scan encrypted payloads in order to detect and prevent threats from attackers.

Networks and devices are often exploited through vulnerabilities. Software vulnerabilities are one such example where a bug or inherent weakness in the code provides attackers an opportunity to gain access to the software. More severe vulnerabilities allow unauthorized access, data leakage, and execution of malicious code. Exploitation of these vulnerabilities can cause damage to the machine and infect others. While the best solution is to patch vulnerabilities as soon as patches are available, IPS signatures offer a solution to detect and block exploitation of many vulnerabilities before they enter the network.

## IPS signatures

Fortinet's solution combines industry-leading threat intelligence from FortiGuard Labs with the FortiGate NGFW to identify the latest threats and prevent them from entering your network. IPS signatures are one such method for delivering the latest protection. FortiGuard Labs uses AI and Machine Learning (ML) to analyze billions of events every day. The FortiGuard Labs research team also proactively performs threat research to discover new vulnerabilities and exploitation, and produces signatures to identify such threats. These IPS signatures are delivered to each FortiGate daily, so that the IPS engine is armed with the latest databases to match the latest threats.

## IPS sensors

A FortiGate IPS sensor is a collection of IPS signatures and filters that define the scope of what the IPS engine will scan when the IPS sensor is applied. An IPS sensor can have multiple sets of signatures and/or filters. A set of IPS signatures consists of manually selected signatures, while a set of IPS filters consists of filters based on signature attributes like target, severity, protocol, OS, and application. Each signature has predefined attributes and an action, such as block, allow, monitor (pass), quarantine, and reset. It is also possible to create custom IPS signatures to apply to an IPS sensor.

From the *Security Profiles > Intrusion Prevention* pane, you can create new IPS sensors and view a list of predefined sensors.

FortiOS includes the following predefined IPS sensors with associated predefined signatures:

Predefined IPS sensors	Description
all_default	Filters all predefined signatures, and sets action to the signature's default action.
all_default_pass	Filters all predefined signatures, and sets action to pass/monitor.
default	Filters all predefined signatures with severity of Critical/High/Medium. Sets action to signature's default action.
high_security	Filters all predefined signatures with severity of Critical/High/Medium, and sets action to Block. For Low severity signatures, sets action to signature's default action.
protect_client	Protects against client-side vulnerabilities by filtering on <code>Target=Client</code> . Sets action to signature's default action.
protect_email_server	Protects against email server-side vulnerabilities by filtering on <code>Target=Server</code> and <code>Protocol=IMAP, POP3 or SMTP</code> . Sets action to signature's default action.

Predefined IPS sensors	Description
protect_http_server	Protects against HTTP server-side vulnerabilities by filtering on <code>Target=Server</code> and <code>Protocol=HTTP</code> . Sets action to signature's default action.
wifi-default	Filters all predefined signatures with severity of Critical/High/Medium. Sets action to signature's default action. Used in profile for offloading WiFi traffic.

## DDoS attacks

Besides protecting against threats and exploitation of vulnerabilities, the IPS engine is also responsible for mitigating Denial of Service (DoS) attacks where attackers attempt to bring a service down by flooding the target with traffic from distributed systems. Using anomaly-based defense, FortiGate can detect a variety of L3 and L4 anomalies and take action against these attacks. This can be configured under IPv4 and IPv6 DoS Policies, which is discussed in detail under [DoS protection on page 822](#).

This section contains the following topics:

- [Signature-based defense on page 1030](#)
- [IPS configuration options on page 1033](#)

This section also provides the following examples about IPS sensors:

- [Botnet C&C IP blocking on page 1037](#)

## Signature-based defense

Signature-based defense is used against known attacks or vulnerability exploits. These often involve an attacker attempting to gain access to your network. The attacker must communicate with the host in an attempt to gain access, and this communication includes commands or sequences of commands and variables. The IPS signatures include these command sequences, allowing the FortiGate unit to detect and stop the attack.

This section describes the following components used in signature-based defense:

- [IPS signatures on page 1030](#)
- [Protocol decoders on page 1031](#)
- [IPS engine on page 1031](#)
- [IPS sensors on page 1031](#)
- [IPS filters on page 1032](#)
- [Custom and predefined signature entries on page 1033](#)
- [Policies on page 1033](#)

## IPS signatures

IPS signatures are the basis of signature-based intrusion prevention. Every attack can be reduced to a particular string of commands or a sequence of commands and variables. Signatures include this information, and FortiGate uses the information to detect and stop attacks.

Signatures also include characteristics about the attack they describe. These characteristics include the network protocol associated with the attack, the vulnerable operating system, and the vulnerable application.

To view the complete list of signatures, go to *Security Profiles > IPS Signatures*. The list of signatures includes predefined and custom signatures. You can hover over the name of the IPS signature to display a pop-up window that includes an ID number. You can click the ID number to display the FortiGuard page.

## Protocol decoders

Before examining network traffic for attacks, the IPS engine uses protocol decoders to identify each protocol appearing in the traffic. Attacks are protocol-specific, so your FortiGate unit conserves resources by looking for attacks only in the protocols used to transmit them. For example, the FortiGate unit will only examine HTTP traffic for the presence of a signature describing an HTTP attack.

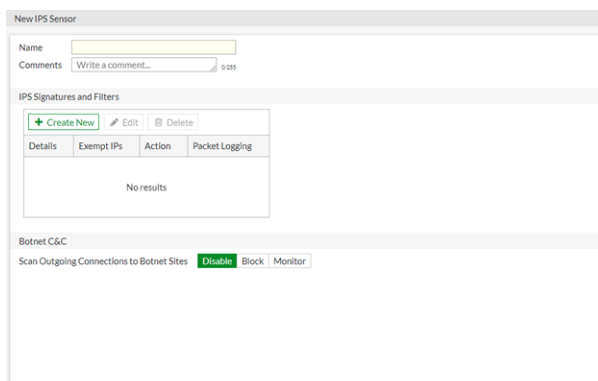
## IPS engine

Once the protocol decoders separate the network traffic by protocol, the IPS engine examines the network traffic for the attack signatures by using IPS sensors.

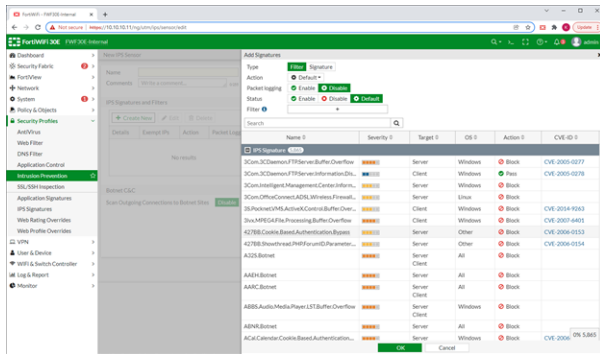
## IPS sensors

The IPS engine does not examine network traffic for all signatures. The IPS engine examines network traffic for signatures specified in IPS sensors. You must first create an IPS sensor, and then you can specify what signatures the IPS sensor will use. You can add individual signatures to IPS sensors, or you can add filters to IPS sensors, and the filters automatically include the applicable signatures.

To view IPS sensors, go to *Security Profiles > Intrusion Prevention*. To create a new sensor, click *Create New*.



An IPS sensor is composed of IPS signatures and filters. Under *IPS Signatures and Filters*, click *Create New* to create a set of IPS signatures or a set of IPS filters.



You can create IPS sensors for specific types of traffic, and then select the IPS sensors in firewall policies designed to handle the same type of traffic. For example, you can specify all of the web-server related signatures in an IPS sensor, and select the IPS sensor in a firewall policy that controls all traffic to and from a web server that is protected by the FortiGate unit.

The FortiGuard Service periodically adds new predefined signatures to counter new threats. New predefined signatures are automatically included in IPS sensors that are configured to use filters when the new signatures match existing filter specifications. For example, if you have an IPS sensor with a filter that includes all signatures for the Windows operating system, your filter will automatically incorporate new Windows signatures that the FortiGuard Service adds to the database.

IPS signature and filter entries are checked from top down. When a signature is found in a set of signatures or filters, the action defined for the signature is taken.

## IPS filters

IPS sensors can contain one or more IPS filters. A filter is a collection of signature attributes that you specify. The signatures that have all of the attributes specified in a filter are included in the IPS filter.

Following are the attribute groups:

- Target
- Severity
- Protocol
- OS
- Application

When selecting multiple attributes within the same group, the selections are combined by using a logical **OR**. When selecting multiple attributes between attribute groups, each attribute group is combined by using a logical **AND**.

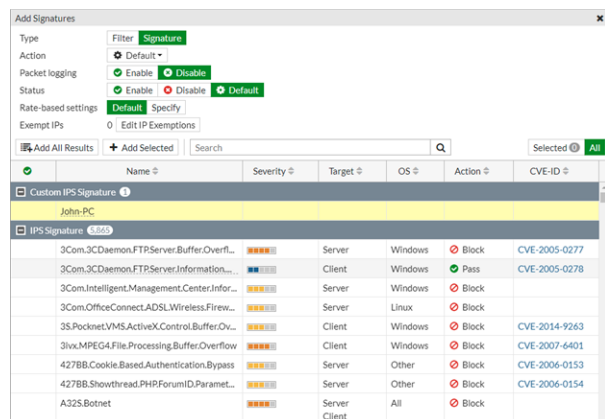
Once you select filters in the GUI, the filtered list of IPS signatures are displayed. Adjust your filters accordingly to construct a suitable list for your needs.

For example, if your FortiGate unit protects a Linux server running the Apache web server software, you could create a new filter to protect it. By setting OS filter attribute to *Linux*, and the filter attribute *Application* to *Apache*, the filter will include only the signatures that apply to both Linux and Apache. If you wanted to scan for all the Linux signatures and all the Apache signatures, you would create two filters, one for each.

To view the filters in an IPS sensor, go to *Security Profiles > Intrusion Prevention*, select the IPS sensor, and click *Edit*.

## Custom and predefined signature entries

Signature entries allow you to add individual, custom or predefined IPS signatures to an IPS sensor. If you need only one signature, or you want to manually select multiple signatures that don't fall into the criteria for an IPS filter, adding a signature entry to an IPS sensor is the easiest way. Signature entries are also the only way to include custom signatures in an IPS sensor.



To select an individual signature, click a signature, and select *Add Selected*. The signature moves to the *Selected* list.

To select multiple signatures, use the *Search* bar to perform a keyword search, and then click *Add All Results* to move all entries to the *Selected* list.

## Overriding the default action

Each IPS signature comes with a default action such as *Block* and *Pass*. In some scenarios, you may want to override this action. You can override a set of IPS filter or signatures. By default, a set of IPS filter or signatures has an action of *Default*, which applies a signature's default action when the signature is matched. By changing the action, you can override the setting for all signatures within the filter or signature set.

## Policies

You must select an IPS sensor in a security policy or an interface policy to apply the IPS sensor to traffic. An IPS sensor that it not selected in a policy is not applied to network traffic.

## IPS configuration options

Besides configuring an IPS filter or selecting IPS signatures for an IPS sensor, you can configure additional IPS options for each sensor or globally for all sensors. This topic introduces the following available configuration options:

- [Malicious URL database for drive-by exploits detection on page 1034](#)
- [IPS signature rate count threshold on page 1034](#)
- [Botnet C&C on page 1035](#)
- [Hardware acceleration for flow-based security profiles \(NTurbo and IPSA\) on page 1035](#)
- [Extended IPS database on page 1035](#)
- [IPS engine-count on page 1035](#)
- [Industrial signature database on page 1036](#)

- [Fail-open on page 1036](#)
- [IPS buffer size on page 1036](#)
- [Session count accuracy on page 1037](#)
- [Protocol decoders on page 1037](#)

## Malicious URL database for drive-by exploits detection

This feature uses a local malicious URL database on the FortiGate to assist in detection of drive-by exploits, such as adware that allows automatic downloading of a malicious file when a page loads without the user's detection. The database contains all malicious URLs active in the last one month, and all drive-by exploit URLs active in the last three months. The number of URLs controlled are in the one million range.

This feature can be enabled from a IPS Sensor in the GUI by going to *Security Profiles > Intrusion Prevention* and editing or creating an IPS Sensor. Then enable *Block malicious URLs*.

From the CLI:

```
config ips sensor
 edit <profile>
 set block-malicious-url [enable | disable]
 next
end
```



Blocking malicious URLs is not supported on some FortiGate models, such as FortiGate 51E, 50E, or 30E.

---

## IPS signature rate count threshold

You can use the IPS signature rate-based settings to specify a rate count threshold that must be met before the signature is triggered. A rate count threshold provides a more controlled recording of attack activity. For example, if multiple login attempts produce a failed result over a short period of time, then an alert would be sent and traffic might be blocked, which is a more manageable response than sending an alert every time a login fails.

This can be configured from the GUI by going to *Security Profiles > Intrusion Prevention*. Create or edit an IPS sensor. Within the sensor, edit the IPS signatures and filters. Only IPS signatures have the rate-based settings option. IPS filters do not.

Some settings are only available from CLI.

The syntax for this configuration is as follows:

```
config ips sensor
 edit default
 config entries
 edit <Filter ID number>
 set rule <*id>
 set rate-count <integer between 1 - 65535>
 set rate-duration <integer between 1 - 65535>
```

The value of the rate-duration is an integer for the time in seconds.

```
set rate-mode <continuous | periodical>
```

The rate-mode refers to how the count threshold is met.



If the setting is “continuous”, and the action is set to block, the action is engaged as soon as the rate-count is reached. For example, if the count is 10, the traffic would be blocked as soon as the signature is triggered 10 times.

If the setting is “periodical”, the FortiGate allows up to the value of the rate-count incidents where the signature is triggered during the rate-duration. For example, if the rate count is 100 and the duration is 60, the signature would need to be triggered 100 times in 60 seconds for the action to be engaged.

```
set rate-track <dest-ip | dhcp-client-mac | dns-domain | none | src-ip>
```

This setting allows the tracking of one of the protocol fields within the packet.

## Botnet C&C

See [Botnet C&C IP blocking on page 1037](#).

## Hardware acceleration for flow-based security profiles (NTurbo and IPSA)

Some FortiGate models support a feature call NTurbo that can offload flow-based firewall sessions to network processors.

Some FortiGate models also support offloading enhanced pattern matching for flow-based security profiles to CP8 or CP9 content processors. You can use the following command to configure NTurbo and IPSA:

```
config ips global
 set np-accel-mode {none | basic}
 set cp-accel-mode {none | basic | advanced}
end
```

If the `np-accel-mode` option is available, your FortiGate supports NTurbo. The `none` option disables NTurbo, and `basic` (the default) enables NTurbo.

If the `cp-accel-mode` option is available, your FortiGate supports IPSA. The `none` option disables IPSA, and `basic` enables basic IPSA, and `advanced` enables enhanced IPSA, which can offload more types of pattern matching than basic IPSA. The `advanced` option is only available on FortiGate models with two or more CP8 processors, or one or more CP9 processors.

## Extended IPS database

Some models have access to an extended IPS Database. Because the extended database may affect FortiGate performance, the extended database package may be disabled by default on some models, such as desktop models.

You can only enable the extended IPS database by using the CLI.

```
config ips global
 set database extended
end
```

## IPS engine-count

FortiGate units with multiple processors can run one or more IPS engine concurrently. The engine-count CLI command allows you to specify how many IPS engines to use at the same time:

```
config ips global
 set engine-count <int>
```

end

The recommended and default setting is 0, which allows the FortiGate unit to determine the optimum number of IPS engines.

## Industrial signature database

Industrial signatures are defined to protect Industrial Control Systems (ICS), Operational Technology (OT) and SCADA systems, which are critical infrastructure used by manufacturing industries. These signatures are enabled by default, but can be configured by using the following CLI:

```
config ips global
 set exclude-signatures {none* | industrial}
end
```

## Fail-open

A fail-open scenario is triggered when IPS raw socket buffer is full. Therefore IPS engine has no space in memory to create more sessions and needs to decide whether to drop the sessions or bypass the sessions without inspection.

```
config ips global
 set fail-open {enable | disable}
end
```

The default setting is `disable`, so sessions are dropped by IPS engine when the system enters fail-open mode.

When enabled, the IPS engine fails open, and it affects all protocols inspected by FortiOS IPS protocol decoders, including but not limited to HTTP, HTTPS, FTP, SMTP, POP3, IMAP, and so on. When the IPS engine fails open, traffic continues to flow without IPS scanning.



Sessions offloaded to Nturbo do not support fail-open. When Nturbo data path is overloaded, traffic is dropped regardless of fail-open setting.

---

## IPS buffer size

If system enters fail-open mode frequently, it is possible to increase the IPS socket buffer size to allow more data buffering, which reduces the chances of overloading the IPS engine. You can set the size of the IPS buffer.

```
config ips global
 set socket-size <int>
end
```

The default socket size and maximum configurable value varies by model. In short, socket-size determines how much data the kernel passes to the IPS engine each time the engine samples packets.

Take caution when modifying the default value. If the socket-size is too large, the higher memory used by the IPS engine may cause the system to enter conserve mode more frequently. If set too low, the system may enter IPS fail-open mode too frequently.

## Session count accuracy

The IPS engine can track the number of open session in two ways. An accurate count uses more resources than a less accurate heuristic count.

```
config ips global
 set session-limit-mode {accurate | heuristic}
end
```

The default is `heuristic`.

## Protocol decoders

The FortiGate Intrusion Prevention system uses protocol decoders to identify the abnormal traffic patterns that do not meet the protocol requirements and standards. For example, the HTTP decoder monitors traffic to identify any HTTP packets that do not meet the HTTP protocol standards.

To change the ports a decoder examines, you must use the CLI. In this example, the ports examined by the DNS decoder are changed from the default 53 to 100, 200, and 300.

```
config ips decoder dns_decoder
 config parameter "port_list"
 set value "100,200,300"
 end
end
```

You cannot assign specific ports to decoders that are set to *auto* by default. These decoders can detect their traffic on any port. Specifying individual ports is not necessary.

## Botnet C&C IP blocking

The *Botnet C&C* section consolidates multiple botnet options in the IPS profile. This allows you to enable botnet blocking across all traffic that matches the policy by configuring one setting in the GUI, or by the `scan-botnet-connections` option in the CLI.

### To configure botnet C&C IP blocking using the GUI:

1. Go to *Security Profiles > Intrusion Prevention*.
2. Edit an existing sensor, or create a new one.

### 3. Set *Scan Outgoing Connections to Botnet Sites* to *Block* or *Monitor*.

4. Configure other settings as required .

5. Click *Apply*. Botnet C&C is now enabled for the sensor.

6. Add this sensor to the firewall policy.

The IPS engine will scan outgoing connections to botnet sites. If you access a botnet IP, an IPS log is generated for this attack.

7. Go to *Log & Report > Intrusion Prevention* to view the log.

#### To configure botnet C&C IP blocking using the CLI:

```
config ips sensor
 edit "Demo"
 set scan-botnet-connections {block | monitor}
 next
end
```



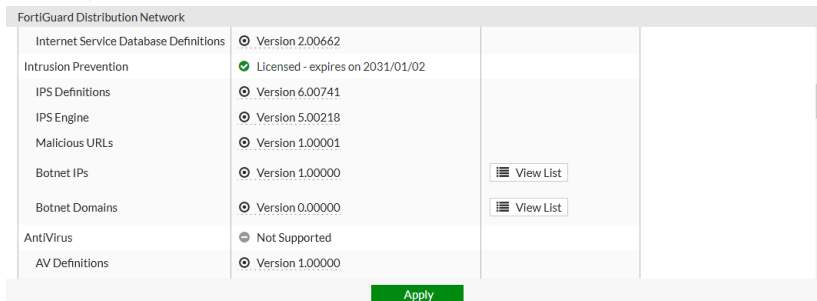
The `scan-botnet-connections` option is no longer available in the following CLI commands:

- `config firewall policy`
- `config firewall interface-policy`
- `config firewall proxy-policy`
- `config firewall sniffer`

## Botnet IPs and domains lists

To view botnet IPs and domains lists using the GUI:

1. Go to *System > FortiGuard*. *Botnet IPs* and *Botnet Domains* are visible in the *Intrusion Prevention* section.

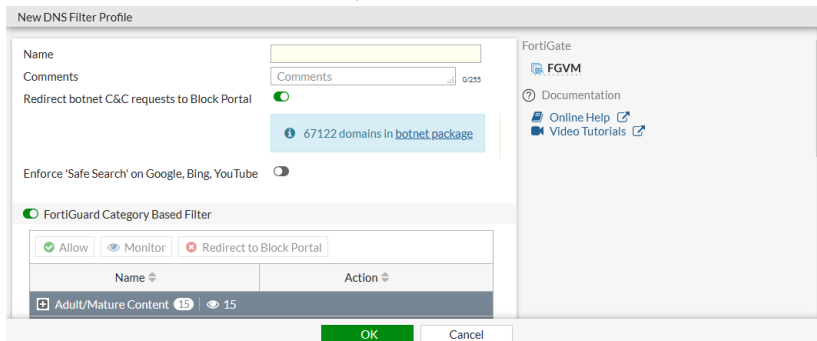


2. Click *View List* for more details.

## Botnet C&C domain blocking

To block connections to botnet domains using the GUI:

1. Go to *Security Profiles > DNS Filter*.
2. Edit an existing filter, or create a new one.
3. Enable *Redirect botnet C&C requests to Block Portal*.



4. Configure other settings as required.
5. Click **OK**.
6. Add this filter profile to a firewall policy.

## Botnet C&C URL blocking

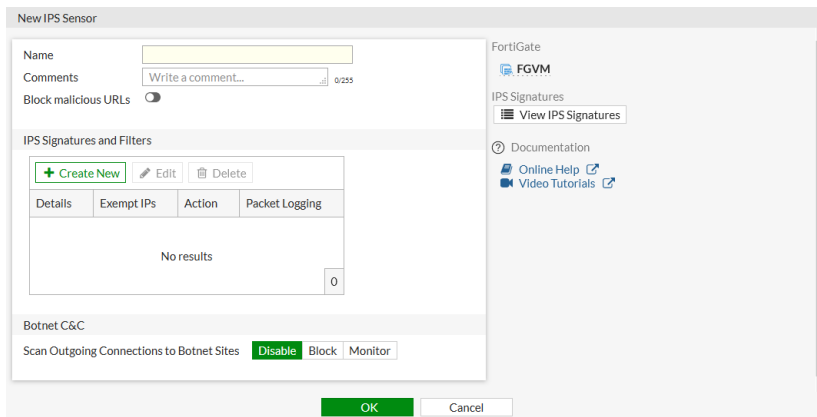


Blocking malicious URLs is not supported on FortiGate 51E, 50E, or 30E models.

To block malicious URLs using the GUI:

1. Go to *Security Profiles > Intrusion Prevention*.
2. Edit an existing sensor, or create a new one.

### 3. Enable *Block malicious URLs*.

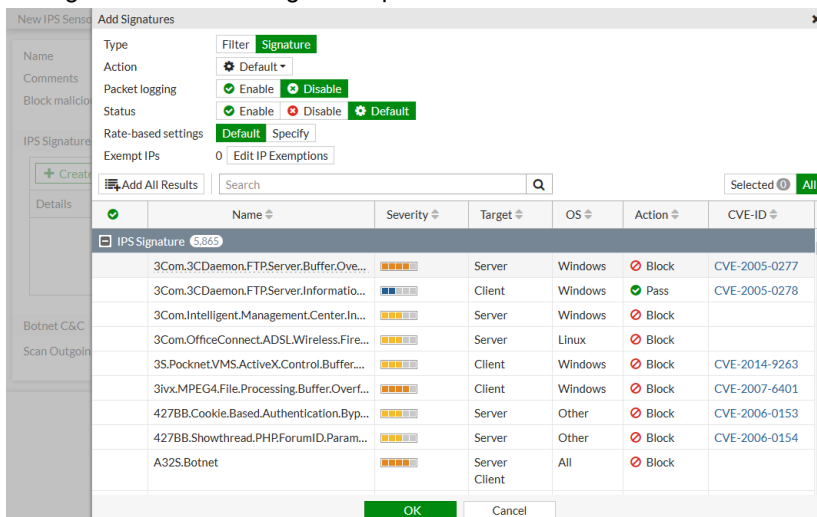


4. Configure other settings as needed.
5. Click **OK**.
6. Add this sensor to a firewall policy.

## Botnet C&C signature blocking

To add IPS signatures to a sensor using the GUI:

1. Go to *Security Profiles > Intrusion Prevention*.
2. Edit an existing sensor, or create a new one.
3. In the *IPS Signatures* section, click *Create New*.
4. Set *Type* to *Signature*.
5. Select the signatures you want to include from the list.
6. Configure the other settings as required.



7. Click **OK**.
8. Configure other settings as required, then click **OK**.
9. Add this sensor to a firewall policy to detect or block attacks that match the IPS signatures.

## Email filter

Email filters can be configured to perform spam detection and filtering. You can customize the default profile, or create your own and apply it to a firewall policy.



Two kinds of filtering can be defined in a single profile, and they will act independent of one another.

---

Filter options can be organized according to the source of the decision:

- Local options: the FortiGate qualifies the email based on local conditions, such as blocklists and allowlists, banned words, or DNS checks using FortiGuard Antispam.
- FortiGuard-based options: the FortiGate qualifies the email based on the score or verdict returned from FortiGuard Antispam.
- Third-party options: the FortiGate qualifies the email based on information from a third-party source (like an ORB list).

Local and FortiGuard block/allowlists can be enabled and combined in a single profile. When combined, the local block/allowlist has a higher priority than the FortiGuard blocklist during a decision making process. For example, if a client IP address is blocklisted in the FortiGuard server, but you want to override this decision and allow the IP to pass through the filter, you can define the IP address or subnet in a local block/allowlist with the *clear* action. Because the information coming from the local list has a higher priority than the FortiGuard service, the email will be considered clean.



Some features of this functionality require a subscription to FortiGuard Antispam.

---

The following topics provide information about email filter profiles:

- [HELO DNS lookup on page 1042](#)
- [FortiGuard-based filters on page 1048](#)
- [Third-party-based filters on page 1050](#)
- [File type-based filters on page 1050](#)
- [Filtering order on page 1056](#)
- [Protocols and actions on page 1057](#)
- [Configuring webmail filtering on page 1058](#)

There are six types of local spam filters:

- [HELO DNS lookup](#)
- [Return email DNS check](#)
- [Block/allow list](#)
- [Banned words](#)\*
- [Trusted IP addresses](#)\*
- [MIME header](#)\*

\* These filters can only be configured in the CLI.



By default, HELO DNS and return email DNS checks are done before the block/allow list check. In some situations, such as when configuring a block/allow list to clear an email from performing further filtering, configure the following to give precedence to the block/allow list:

```
config emailfilter profile
 edit <name>
 config smtp
 set local-override enable
 next
 end
end
```

## HELO DNS lookup

Whenever a client opens an SMTP session with a server, the client sends a HELO command with the client domain name. The FortiGate takes the domain name specified by the client in the HELO and performs a DNS lookup to determine if the domain exists. If the lookup fails, the FortiGate determines that any emails delivered during the SMTP session are spam. The HELO DNS lookup is only available for SMTP traffic.

## Return email DNS check

The FortiGate performs a DNS lookup on the return field. If no such record exists, the email is treated as spam. When return email DNS checking is enabled, the FortiGate takes the domain in the reply-to email address and reply-to domain, and checks the DNS servers to see if there is an A or MX record for the domain. If the domain does not exist, the FortiGate treats the email as spam.

## Block/allow list

Block/allow lists can be made from emails or IP subnets to forbid or allow them to send or receive emails. The following table summarizes the configurable options in a block/allow list.

Type	Description	Pattern	Action
<i>IP/Netmask</i> and <i>IPv6/Netmask</i>	<p>The FortiGate compares the IP address of the client delivering the email to the addresses in the IP address block/allow list specified in the email filter profile.</p> <p>If a match is found, the FortiGate takes the action configured for the matching block/allow list entry against all delivered email.</p> <p>By default the <code>hdrrip</code> setting under <code>config smtp</code> is disabled. If enabled, the FortiGate checks all the IP addresses in the header of SMTP email against the specified IP address block/allow list.</p>	The filter is an IP address with a subnet mask.	<ul style="list-style-type: none"> <li><i>Mark as Reject:</i> the email is dropped before reaching its destination.</li> <li><i>Mark as Spam:</i> the email is allowed through, but it will be tagged</li> </ul>



Type	Description	Pattern	Action
<i>Email Regular Expression</i>	The FortiGate compares the sender email address, as shown in the email envelope MAIL FROM, to the pattern in the patterned field. If a match is found, the FortiGate takes the action configured for the matching block/allow list entry.	The filter is a regular expression. For example, <code>^[a-z0-9-]+(\.[a-z0-9-]+)*@(example xmp examp).com org net</code> can be used to filter based on a number of email domain name combinations.	with an indicator marking the email as spam. • <i>Mark as Clear:</i> the email is allowed to go through to its destination on the assumption that it is not spam.
<i>Email Wildcard</i>	The FortiGate compares the sender email address, as shown in the email header and envelope MAIL FROM, to the pattern in the patterned field. If a match is found, the FortiGate takes the action configured for the matching block/allow list entry.	The filter is an email address with a wildcard symbol in place of the variable characters (such as <code>*.example.com</code> or <code>fred@*.com</code> ).	

## Banned words

When banned word checking is enabled, the FortiGate examines emails for words that appear in the banned word list specified in the email filter profile.

The banned word pattern can be either wildcard or Perl regular expression, which could include part of a word, a whole word, a phrase, multiple words, or multiple phrases.

Each time the banned word filter detects a pattern in an email, it adds the pattern score to the sum of scores for the message. The score is set when creating a new pattern to block content (`set score`). Higher scores indicate more offensive content. If the total score of the discovered banned words in the email exceeds the threshold value set in the email filter profile, then the FortiGate treats the email as spam. The score for each pattern is counted only once, even if that pattern appears many times in the email. The default score for banned word patterns is 10, and the default threshold in the email filter is 10. This means that by default, an email message is blocked by a single match.

For example, if the FortiGate scans an email containing only this sentence: “The score for each word or phrase is counted only once, even if that word or phrase appears many times in the email message.” and the banned word list contains the following patterns:

Banned word pattern	Pattern type	Assigned score	Score added to sum for entire page	Comments
word	Wildcard	20	20	The pattern appears twice, but it is counted once.
word phrase	Wildcard	20	0	Both words appear in the email, but they do not appear together as specified in the pattern. There are no matches.

Banned word pattern	Pattern type	Assigned score	Score added to sum for entire page	Comments
word*phrase	Wildcard	20	20	A match occurs as long as “word” appears before “phrase” regardless of what is in between them. The pattern appears twice, but it is counted once.
mail*age	Wildcard	20	20	This pattern is a match because “email message” appears in the email.

The email would be treated as spam if the banned word threshold is set to 60 or less.

### To apply a banned word filter to an email filter profile:

#### 1. Configure the banned words list:

```
config emailfilter bword
 edit 1
 set name "banned"
 config entries
 edit 23
 set pattern-type {wildcard | regexp}
 set pattern <string>
 set score <1 - 99999>
 next
 end
 next
end
```

#### 2. Configure the email filter profile:

```
config emailfilter profile
 edit "myBannedWordsProfile"
 set spam-filtering enable
 set options bannedword
 set spam-bword-threshold <0 - 2147483647>
 set spam-bword-table 23
 next
end
```



Once a banned word list is configured in the CLI and applied to an email filter profile, some settings can be edited in the GUI for that particular email filter profile. A banned word profile can be selected, and its *Threshold* (spam-bword-threshold) can be edited.

## Trusted IP addresses

When the FortiGate creates a list of trusted IP addresses, any incoming email traffic from these IP address is exempt from having IP-based checks, such as DNSBL, RBL, FortiGuard Antispam service, or locally-defined IP block lists.

If the FortiGate sits behind a company's mail transfer units, it may be unnecessary to check email IP addresses because they are internal and trusted. In this case, only external IP addresses would be checked. In some cases, external IP addresses may be added to the list if they are known to not be spam sources.

### To configure a trusted IP address list:

#### 1. Define the IP address list:

```
config emailfilter iptrust
 edit 1
 set name "trustedIP"
 config entries
 edit 33
 set addr-type {ipv4 | ipv6}
 set ipv4-subnet <IPv4_classnet>
 set ipv6-subnet <IPv6_network>
 next
 end
 next
end
```

#### 2. Add the list to the email filter profile:

```
config emailfilter profile
 edit "email_filter_profile"
 set spam-iptrust-table 1
 next
end
```

## MIME header

This feature filters by the MIME header.

### To configure a MIME header check:

#### 1. Define the header content:

```
config emailfilter mheader
 edit 100
 set name "mheader"
 config entries
 edit 1
 set fieldname <string>
 set fieldbody <string>
 set pattern-type {wildcard | regexp}
 set action {spam | clear}
 next
 end
 next
end
```

#### 2. Add the header to the email filter profile:

```
config emailfilter profile
 edit "email_filter_profile"
 set options spamhdrcheck
```

```

 set spam-mheader-table 100
 next
end

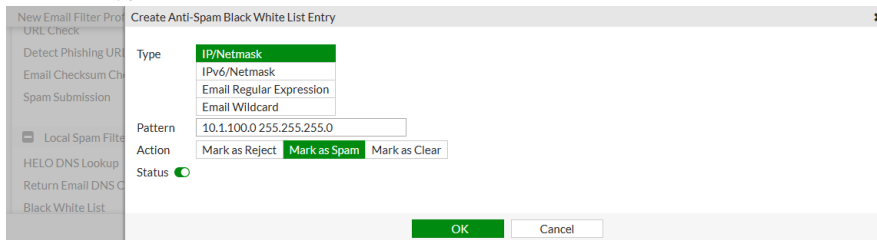
```

## Configuring a local-based email filter

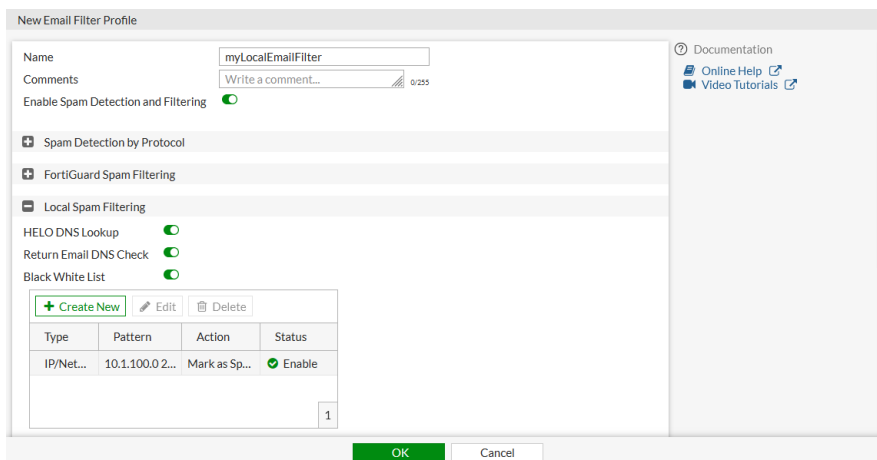
To configure a local-based email filter in the GUI:

1. Configure the email filter profile:

- a. Go to *Security Profiles > Email Filter* and click *Create New*, or edit an existing profile.
- b. Select a *Feature set* (*Proxy-based* is used in this example) and enable *Enable Spam Detection and Filtering*.
- c. In the *Local Spam Filtering* section, enable the desired filters (*HELO DNS Lookup*, *Return Email DNS Check*, *Black White List*).
- d. If *Black White List* is enabled, click *Create New*. The *Create Anti-Spam Black White List Entry* pane opens.
- e. Select a *Type*, enter a *Pattern*, and select an *Action*.



f. Click *OK* to save the block/allow list.

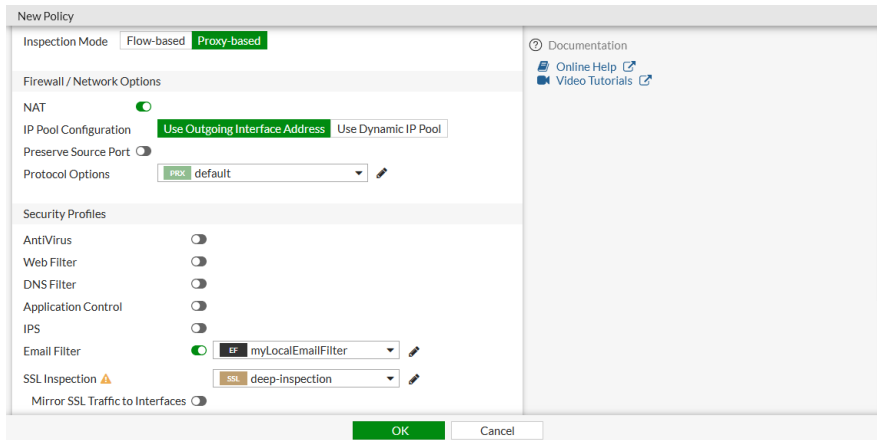


g. Click *OK* save the email filter profile.

2. Configure the firewall policy:

- a. Go to *Policy & Objects > Firewall Policy* and click *Create New*, or edit an existing policy.
- b. Set the inspection-mode to *Proxy-based*.

- c. Enable the *Email Filter* option and select the previously created profile.



- d. Set *SSL Inspection* to a profile that has deep SSL inspection enabled.  
Deep inspection is required to filter SMTP, POP3, IMAP, or any SSL/TLS encapsulated protocol.
- e. Configure the other settings as needed.
- f. Click **OK**.

### To configure a local-based email filter in the CLI:

1. Configure a block/allow list:

```
config emailfilter bwl
 edit 1
 set name "myBAL"
 config entries
 edit 1
 set status enable
 set type ip
 set action spam
 set addr-type ipv4
 set ip4-subnet 10.1.100.0 255.255.255.0
 next
 end
 next
end
```

2. Configure an email filter profile:

```
config emailfilter profile
 edit "myLocalEmailFilter"
 set spam-filtering enable
 set options spambwl spamhelodns spamraddrdns
 config smtp
 set action tag
 end
 set spam-bwl-table 1
 next
end
```

3. Use the profile in a firewall policy:

```
config firewall policy
 edit 1
```

```
 set inspection-mode proxy
 set emailfilter-profile "myLocalEmailFilter"
 next
end
```

## FortiGuard-based filters

The FortiGate consults FortiGuard servers to help identify spammer IP address or emails, known phishing URLs, known spam URLs, known spam email checksums, and others. For more information, refer to the [FortiGuard](#) website.

There are five FortiGuard spam filtering options:

- [IP address check](#)
- [URL check](#)
- [Detect phishing URLs in email](#) (requires URL check to be enabled)
- [Email checksum check](#)
- [Spam submission](#)

### IP address check

The FortiGate queries the FortiGuard Antispam service to determine if the IP address of the client delivering the email is in the block list. If there is a match, the FortiGate treats delivered emails as spam.

### URL check

The FortiGate submits all URLs that appear in the email body to the FortiGuard service for checking. If a URL exists in the FortiGuard URL block list, the FortiGate treats the email as spam.

### Detect phishing URLs in email

The FortiGate submits all URL hyperlinks that appear in the email body to the FortiGuard service for checking. If a URL exists in the FortiGuard URL phishing list, the FortiGate removes the hyperlink from the message. The URL remains in place, but it is no longer a clickable hyperlink.

### Email checksum check

The FortiGate submits a checksum of each email to the FortiGuard service for checking. If a checksum exists in the FortiGuard checksum block list, the FortiGate treats the email as spam.

### Spam submission

Spam submission is a way to inform the FortiGuard Antispam service of non-spam messages incorrectly marked as spam. When enabled, the FortiGate adds a link to the end of every email marked as spam. Click the link to notify the FortiGuard Antispam service if an email is marked incorrectly.

## Configuring FortiGuard filters

### To configure FortiGuard filters in the GUI:

1. Go to *Security Profiles > Email Filter* and click *Create New*.
2. Enable *Enable Spam Detection and Filtering*.
3. In the *FortiGuard Spam Filtering Spam Filtering* section, enable the following as needed:
  - *IP Address Check*
  - *URL Check*
  - *Detect Phishing URLs in Email*
  - *Email Checksum Check*
  - *Spam Submission*

Protocol	Spam Action	Tag Location	Tag Format
IMAP	Tag	Subject	Spam
POP3	Tag	Subject	Spam
SMTP	Discard	Subject	Spam

**FortiGuard Spam Filtering**

- IP Address Check ☒
- URL Check ☒
- Detect Phishing URLs in Email ☒
- Email Checksum Check ☒
- Spam Submission ☒

**Local Spam Filtering**

OK Cancel

4. Click *OK*.

### To configure FortiGuard filters in the CLI:

```
config emailfilter profile
 edit <name>
 set spam-filtering enable
 set options spamfsip spamfsurl spamfsphish spamfschksum spamfssubmit
 next
end
```

Option	Description
spamfsip	Check email IP addresses
spamfsurl	Check email content URLs
spamfsphish	Check email content phishing URLs
spamfschksum	Check email checksums
spamfssubmit	Add FortiGuard Antispam spam submission text

## Third-party-based filters

In addition to local and FortiGuard filters, FortiOS can leverage third-party sources, which are known as DNS-based blackhole lists (DNSBL) or Open Relay Behavior-modification Systems (ORBS). These are maintained lists of IP addresses that have been identified as associated with spamming.

The following example demonstrates how to configure a DNSBL. The `config emailfilter dnsbl` command is used to configure either DNSBL or ORBS.

### To configure a DNSBL:

1. Define the server to get the DNSBL list from:

```
config emailfilter dnsbl
 edit 100
 set name "dnsbl"
 config entries
 edit 1
 set status enable
 set server <IP address or server name>
 set action {reject | spam}
 next
 end
 next
end
```

2. Add the DNSBL list to an email filter profile:

```
config emailfilter profile
 edit "email_filter_profile"
 set options spamrbl
 set spam-rbl-table 100
 next
end
```

## File type-based filters

With *File Filter*, you can define undesired file types within the email filter profile and associate an action to be taken for each file type, such as block or log.

For each entry, you can also specify the protocol to inspect (SMTP, POP3, or IMAP) and if only encrypted files should be matched. While file filter entries are ordered, the block action takes precedence over the log action.

File filtering in email filter profiles is based only on the file type (file meta data) and not on file size or content. You would need to configure a DLP sensor to block files based on size or content, such as SSN numbers, credit card numbers, or regexp.

File filtering only works in proxy mode policies. The traffic direction cannot be configured because it is implied by the protocol.

The following file types are supported:



File Type Name	Description
7z	Match 7-zip files
arj	Match arj compressed files
cab	Match Windows cab files
lzh	Match lzh compressed files
rar	Match rar archives
tar	Match tar files
zip	Match zip files
bzip	Match bzip files
gzip	Match gzip files
bzip2	Match bzip2 files
xz	Match xz files
bat	Match Windows batch files
msc	Match msc files
uue	Match uue files
mime	Match mime files
base64	Match base64 files
binhex	Match binhex files
bin	Match bin files
elf	Match elf files
exe	Match Windows executable files
hta	Match hta files
html	Match html files
jad	Match jad files
class	Match class files
cod	Match cod files
javascript	Match javascript files
msoffice	Match MS-Office files. For example, doc, xls, ppt, and so on.
msofficex	Match MS-Office XML files. For example, docx, xlsx, pptx, and so on.
fsg	Match fsg files
upx	Match upx files

File Type Name	Description
petite	Match petite files
aspack	Match aspack files
prc	Match prc files
sis	Match sis files
hlp	Match Windows help files
activemime	Match activemime files
jpeg	Match jpeg files
gif	Match gif files
tiff	Match tiff files
png	Match png files
bmp	Match bmp files
unknown	Match unknown files
mpeg	Match mpeg files
mov	Match mov files
mp3	Match mp3 files
wma	Match wma files
wav	Match wav files
pdf	Match pdf files
avi	Match avi files
rm	Match rm files
torrent	Match torrent files
msi	Match Windows Installer msi bzip files
mach-o	Match Mach object files
dmg	Match Apple disk image files
.net	Match .NET files
xar	Match xar archive files
chm	Match Windows compiled HTML help files
iso	Match ISO archive files
crx	Match Chrome extension files

## Example

In the following example, one file filter entry is created to block executable (exe) files from being sent or received, and a second entry logs any documents that are sent.

### To configure a file-type based email filter in the CLI:

#### 1. Configure an email filter profile:

```
config emailfilter profile
 edit "file-type-filter"
 config file-filter
 set status enable
 set log enable
 set scan-archive-contents enable
 config entries
 edit "filter1"
 set comment "Block executable files"
 set protocol smtp imap pop3
 set action block
 set encryption any
 set file-type "exe"
 next
 edit "filter2"
 set comment "Log document files"
 set protocol smtp
 set action log
 set encryption any
 set file-type "pdf" "msoffice" "msofficex"
 next
 end
 end
 set spam-filtering enable
next
end
```

#### 2. Use the profile in a firewall policy:

```
config firewall policy
 edit 1
 set name "client-to-internet"
 set srcintf "port2"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set utm-status enable
 set utm-inspection-mode proxy
 set logtraffic all
 set emailfilter profile "file-type-filter"
 set profile-protocol-options "protocol"
 set ssl-ssh-profile "protocols"
 set nat enable
```

```
next
end
```

### To view the file filter logs:

```
execute log filter category utm-file-filter
execute log display
```

#### File filter block action:

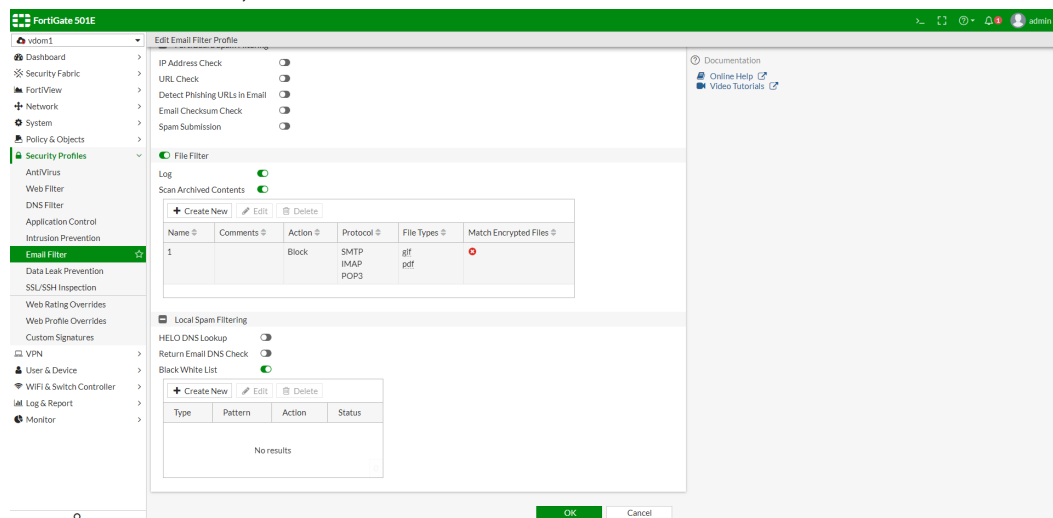
```
1: date=2019-01-25 time=15:20:16 logid="0554020511" type="utm" subtype="file-filter"
eventtype="file-filter" level="warning" vd="vdom1" eventtime=1548458416 policyid=1
sessionid=2881 srcip=10.1.100.12 srcport=45974 srcintf="port2" srcintfrole="undefined"
dstip=172.16.200.56 dstport=143 dstintf="port1" dstintfrole="undefined" proto=6
service="IMAP" action="blocked" from="emailuser1@qa.fortinet.com"
to="emailuser2@qa.fortinet.com" recipient="emailuser2" direction="incoming" subject="EXE
file block" size="622346" attachment="yes" filename="putty.exe" filtername="filter1"
filetype="exe"
```

#### File filter log action:

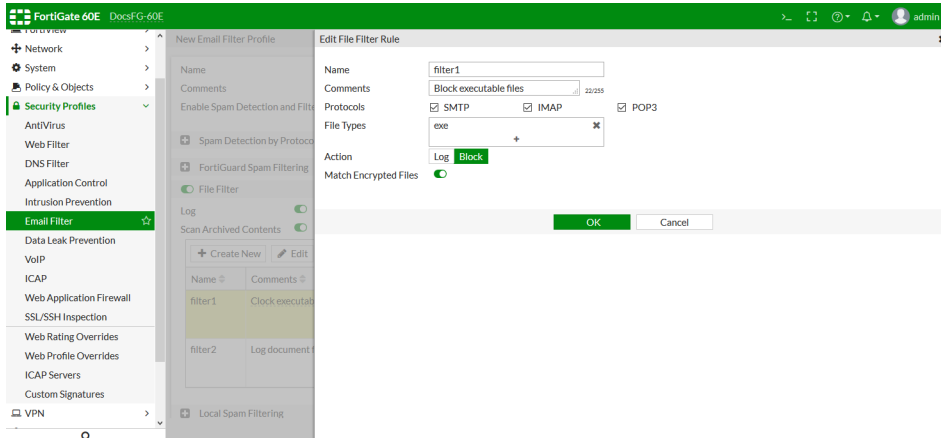
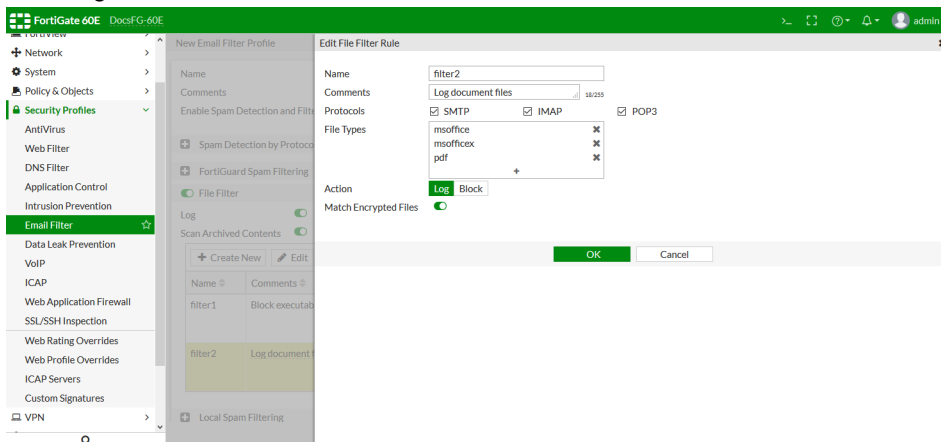
```
1: date=2020-06-25 time=10:56:04 logid="1900064000" type="utm" subtype="file-filter"
eventtype="file-filter" level="warning" vd="root" eventtime=1593050164413818122 tz="+0900"
policyid=1 sessionid=202 srcip=10.0.0.20 srcport=38984 srcintf="port1" srcintfrole="lan"
dstip=10.0.10.20 dstport=110 dstintf="wan1" dstintfrole="wan" proto=6 service="POP3"
profile="default" direction="incoming" action="blocked" from="guest@client.com"
to="aki@fortitest.jp" recipient="aki@fortitest.jp" subject="Test mail" filtername="test"
filename="test.pdf" filesize=24205 filetype="pdf" msg="File was blocked by file filter."
```

### To configure a file-type based email filter in the GUI:

1. Go to *Security Profiles > Email Filter*.
2. Click *Create New*, or select an existing profile and click *Edit*.
3. Enable *Enable Spam Detection and Filtering*.
4. Enable *File Filter*.
5. Enable *Log* and *Scan Archived Contents*.
6. In the *File Filter* table, click *Create New*.

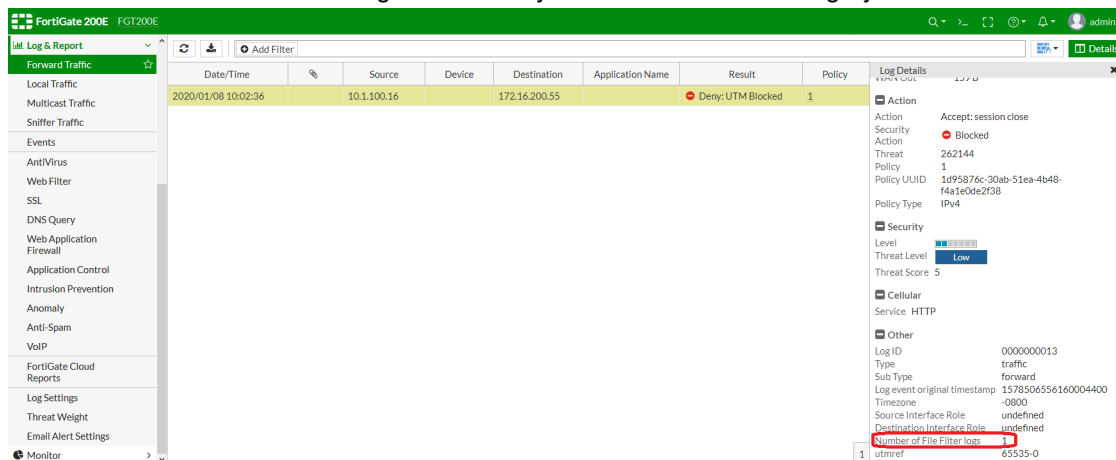


## 7. Configure the filters:

a. *filter1* blocks all sent or received executable files.b. *filter2* logs all sent documents.

## 8. Click OK.

## 9. Add the new email filter profile to a firewall policy.

10. To see if there are file filter logs, go to *VDOM > Log & Report > Forward Traffic*. Select an entry and view the *Log Details*. The number of file filter logs for that entry is listed in the *Other* category.



File filter logs can only be viewed in the CLI.

## Filtering order

The FortiGate checks for spam using various filtering techniques. The filtering order used by the FortiGate depends on which mail protocol is used.

Filters requiring a query to a server and a reply (FortiGuard Antispam service and DNSBL/ORDBL) are run simultaneously. To avoid delays, queries are sent while other filters are running. The first reply to trigger a spam action takes effect as soon as the reply is received.

Each spam filter passes the email to the next if no matches or problems are found. If the action in the filter is *Mark as Spam*, the FortiGate tags the email as spam according to the settings in the email filter profile. If the action in the filter is *Mark as Reject*, the email session is dropped. If the action in the filter is *Mark as Clear*, the email is exempt from any remaining filters. For SMTP and SMTPS, if the action is *Discard*, the email is discarded or dropped.

### SMTP and SMTPS spam filtering order

The FortiGate scans SMTP and SMTPS email for spam in a specific order, which depends on whether or not the local override feature is enabled. This feature is disabled by default, but enabling it gives priority to local spam filters.

You can enable local override (`set local-override`) in an email filter profile to override SMTP or SMTPS remote checks, which includes checks for IP RBL, IP FortiGuard AntiSpam, and HELO DNS with the locally defined antispam block and/or allow lists.



SMTPS spam filtering is available on FortiGates that support SSL content scanning and inspection.

### To configure local override of an antispam filter:

```
config emailfilter profile
 edit <name>
 set spam-filtering enable
 set options spambwl spamfsip spamfsurl spamhelodns spamfsphish
 config smtp
 set local-override {enable | disable}
 end
 set spam-bwl-table 1
 next
end
```

Local override disabled	Local override enabled
<ol style="list-style-type: none"> <li>1. HELO DNS lookup, last hop IP check against ORDBL</li> </ol>	<ol style="list-style-type: none"> <li>1. Last hop IP checks local block/allow list</li> <li>2. Envelope address checks local block/allow list</li> </ol>

Local override disabled	Local override enabled
<ol style="list-style-type: none"> <li>Return email DNS check, FortiGuard email checksum check, FortiGuard URL check, FortiGuard IP address check, phishing URLs detection</li> <li>Last hop IP checks local block/allow list</li> <li>Envelope address checks local block/allow list</li> <li>Headers IPs local block/allow list</li> <li>Headers email address local block/allow list, MIME header checks based on local list of patterns (<code>mheader</code>)</li> <li>Banned words (subject first, then body) based on local block/allow list (<code>bword</code>)</li> </ol>	<ol style="list-style-type: none"> <li>Headers IPs local block/allow list, MIME header checks based on local list of patterns (<code>mheader</code>)</li> <li>Headers email address local block/allow list</li> <li>Banned words (subject first, then body) based on local list of patterns (<code>bword</code>)</li> <li>HELO DNS lookup, last hop IP check against ORDBL</li> <li>Return email DNS check, FortiGuard email checksum check, FortiGuard URL check, FortiGuard IP address check, phishing URLs detection</li> </ol>

## IMAP, IMAPS, POP3, and POP3S spam filtering order

The FortiGate scans IMAP, IMAPS, POP3, and POP3S email for spam in the following order:

- MIME headers check, email address block/allow list check
- Banned word check on email subject
- IP block/allow list check
- Banned word check on email body
- Return email DNS check, FortiGuard email checksum check, FortiGuard URL check, DNSBL and ORDBL checks



IMAPS and POP3S spam filtering are available on FortiGates that support SSL content scanning and inspection.

## Protocols and actions

In an email filtering profile, there are sections for SMTP, POP3, and IMAP protocols. In each section, you can set an action to either discard, tag, or pass the log for that protocol.

Protocol	Available action
SMTP	<b>Pass:</b> Allow spam email to pass through.
	<b>Tag:</b> Tag spam email with configured text in the subject or header.
	<b>Discard:</b> Discards (blocks) spam email.
POP3 & IMAP	<b>Pass:</b> Allow spam email to pass through.
	<b>Tag:</b> Tag spam email with configured text in the subject or header.
MAPI:	<b>Pass:</b> Allow spam email to pass through.
	<b>Discard:</b> Discards (blocks) spam email.

For example, to tag spam SMTP email, use the following commands:

```
config emailfilter profile
 edit "smtpFilter"
 set spam-filtering enable
 set options <options>
 ...
 config smtp
 set log enable
 set action tag
 end
 next
end
```

### MAPI email filtering

MAPI is a proprietary protocol from Microsoft. It uses HTTPS to encapsulate email requests and responses between Microsoft Outlook clients and Microsoft Exchange servers. The configuration of MAPI email filters are only possible through the CLI.

#### To configure the MAPI email filter in the CLI:

```
config emailfilter profile
 edit "myMapiFilter"
 set spam-filtering enable
 set options spamfsip spamfssubmit spamfsurl spamfsphish
 config mapi
 set log enable
 set action "discard or pass"
 end
 next
end
```

### Configuring webmail filtering

You can configure an email filter to detect and log emails sent via Gmail and Hotmail. These interfaces do not use standard email protocols (SMTP, POP3, or IMAP) and instead use HTTPS. However, you can still configure the email filter to detect emails that pass through the FortiGate.



The FortiGate only detects and logs the emails, it does not discard or tag them.

---

#### To configure webmail filtering in the CLI:

```
config emailfilter profile
 edit "myWebMailDetector"
 set spam-filtering enable
 config msn-hotmail
 set log enable
 end
 config gmail
 set log enable
 end
 next
end
```

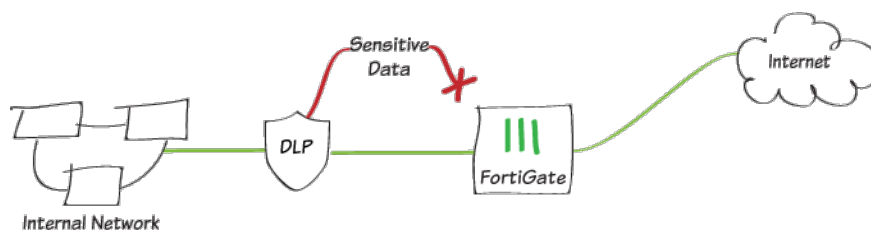


```
 end
 next
end
```

## Data leak prevention

The FortiGate data leak prevention (DLP) system prevents sensitive data from leaving or entering your network. You can customize the default sensor or create your own by adding individual filters based on file type, file size, a regular expression, an advanced rule, or a compound rule. Once configured, you can apply the DLP sensor to a firewall policy. Data matching defined sensitive data patterns is blocked, logged, or allowed when it passes through the FortiGate.

DLP can only be configured in the CLI.



The filters in a DLP sensor can examine traffic for the following:

- Known files using DLP fingerprinting
- Known files using DLP watermarking
- Particular file types
- Particular file names
- Files larger than a specified size
- Data matching a specified regular expression
- Credit card and social security numbers



Filters are ordered, but there is no precedence between the possible actions

DLP is primarily used to stop sensitive data from leaving your network. DLP can also be used to prevent unwanted data from entering your network and to archive some or all of the content that passes through the FortiGate. DLP archiving is configured per filter, which allows a single sensor to archive only the required data. You can configure the DLP archiving protocol in the CLI (see [Configure DLP sensors](#)).

There are two forms of DLP archiving:

- Summary only: a summary of all the activity detected by the sensor is recorded. For example, when an email message is detected, the sender, recipient, message subject, and total size are recorded. When a user accesses the web, every URL that they visit is recorded.
- Full: detailed records of all the activity detected by the sensor is recorded. For example, when an email message is detected, the message itself, including any attachments, is recorded. When a user accesses the web, every page that they visit is archived.

The following topics provide information about DLP:

- [Basic DLP filter types on page 1060](#)
- [DLP fingerprinting on page 1062](#)

## Basic DLP filter types

Basic filter types can be configured in the CLI and include:

- [File type and name](#)
- [File size](#)
- [Regular expression](#)
- [Credit card and SSN](#)

### File type and name

A file type filter allows you to block, allow, log, or quarantine based on the file type specified in the file filter list (see [File filter on page 967](#)).

#### To configure file type and name filtering:

1. Create a file pattern to filter files based on the file name pattern or file type:

```
config dlp filepattern
 edit <filepattern_entry_integer>
 set name <string>
 config entries
 edit <file pattern>
 set filter-type <type | pattern>
 set file-type <file type>
 next
 end
 next
end
```

For example, to filter for GIFs and PDFs:

```
config dlp filepattern
 edit 11
 set name "sample_config"
 config entries
 edit "*.gif"
 set filter-type pattern
 next
 edit "pdf"
 set filter-type type
 set file-type pdf
 next
 end
 next
end
```

2. Attach the file pattern to a DLP sensor, and specify the protocols and actions:

```
config dlp sensor
 edit <string>
```

```
 config filter
 edit <integer>
 set name <string>
 set proto <smtp | pop3 | imap | http-get | http-post | ftp | nntp |
mapi>
 set filter-by file-type
 set file-type l1 <-- Previously configured filepattern
 set action <allow | log-only| block | quarantine-ip>
 next
 end
next
end
```

## File size

A file size filter checks for files that exceed the specific size, and performs the DLP sensor's configured action on them.

### To configure file size filtering:

```
config dlp sensor
 edit <string>
 config filter
 edit <integer>
 set name <string>
 set proto <smtp | pop3 | imap | http-get | http-post | ftp | nntp | mapi>
 set filter-by file-size <-- Match any file over with a size over the
threshold
 set file-type l1 <-- Previously configured filepattern
 set action <allow | log-only| block | quarantine-ip>
 next
 end
 next
end
```

## Regular expression

A regular expression filter is used to filter files or messages based on the configured regular expression pattern.

### To configure regular expression filtering:

```
config dlp sensor
 edit <string>
 config filter
 edit <integer>
 set name <string>
 set type <file | message> <-- Check contents of a file or of messages, web
pages, etc.
 set proto <smtp | pop3 | imap | http-get | http-post | ftp | nntp | mapi>
 set filter-by regexp <-- Use a regular expression to match content
 set regexp <regexp> <-- Input a regular expression pattern
 set action <allow | log-only| block | quarantine-ip>
 next
 end
 end
```

```
 next
end
```

## Credit card and SSN

The credit card sensor can match the credit card number formats used by American Express, Mastercard, and Visa. It can be used to filter files or messages.

The SSN sensor can be used to filter files or messages for Social Security Numbers.

### To configure credit card or SSN filtering:

```
config dlp sensor
 edit <string>
 config filter
 edit <integer>
 set name <string>
 set type <file | message> <-- Check contents of a file, or of messages, web
pages, etc.
 set proto <smtp | pop3 | imap | http-get | http-post | ftp | nntp | mapi>
 set filter-by < credit-card | ssn > <-- Match credit cards or social security
numbers
 set action <allow | log-only| block | quarantine-ip>
 next
 end
 next
end
```

## DLP fingerprinting

DLP fingerprinting can be used to detect sensitive data. The file that the DLP sensor will filter for is uploaded and the FortiGate generates and stores a checksum fingerprint. The FortiGate unit generates a fingerprint for all of the files that are detected in network traffic, and compares all of the checksums stored in its database. If a match is found, the configured action is taken.

Any type of file can be detected by DLP fingerprinting, and fingerprints can be saved for each revision of a file as it is updated.

To use fingerprinting:

- Select the files to be fingerprinted by targeting a document source.
- Add fingerprinting filters to DLP sensors.
- Add the sensors to firewall policies that accept traffic that the fingerprinting will be applied on.



The document fingerprint feature requires a FortiGate device that has internal storage.

---

**To configure a DLP fingerprint document:**

```

config dlp fp-doc-source
 edit <name_str>
 set server-type smb
 set server <string>
 set period {none | daily | weekly | monthly}
 set vdom {mgmt | current}
 set scan-subdirectories {enable | disable}
 set remove-deleted {enable | disable}
 set keep-modified {enable | disable}
 set username <string>
 set password <password>
 set file-path <string>
 set file-pattern <string>
 set sensitivity <Critical | Private | Warning>
 set tod-hour <integer>
 set tod-min <integer>
 set weekday {sunday | monday | tuesday | wednesday | thursday | friday |
saturday}
 set date <integer>
 next
end

```

Command	Description
server-type smb	The protocol used to communicate with document server. Only Samba (SMB) servers are supported.
server <string>	IPv4 or IPv6 address of the server.
period {none   daily   weekly   monthly}	The frequency that the FortiGate checks the server for new or changed files.
vdom {mgmt   current}	The VDOM that can communicate with the file server.
scan-subdirectories {enable   disable}	Enable/disable scanning subdirectories to find files.
remove-deleted {enable   disable}	Enable/disable keeping the fingerprint database up to date when a file is deleted from the server.
keep-modified {enable   disable}	Enable/disable keeping the old fingerprint and adding a new one when a file is changed on the server.
username <string>	The user name required to log into the file server.
password <password>	The password required to log into the file server.
file-path <string>	The path on the server to the fingerprint files.
file-pattern <string>	Files matching this pattern on the server are fingerprinted.
sensitivity <Critical   Private   Warning>	The sensitivity or threat level for matches with this fingerprint database.
tod-hour <integer>	Set the hour of the day. This option is only available when <code>period</code> is not <code>none</code> .

Command	Description
<code>tod-min &lt;integer&gt;</code>	Set the minute of the hour. This option is only available when <code>period</code> is not <code>none</code> .
<code>weekday {sunday   monday   tuesday   wednesday   thursday   friday   saturday}</code>	Set the day of the week. This option is only available when <code>period</code> is <code>weekly</code> .
<code>date &lt;integer&gt;</code>	Set the day of the month. This option is only available when <code>period</code> is <code>monthly</code> .

### To configure a DLP fingerprint sensor:

```

config dlp sensor
 edit <sensor name>
 config filter
 edit <id number of filter>
 set proto {smtp | pop3 | imap http-get | http-post | ftp | nntp | mapi}
 set filter-by fingerprint
 set sensitivity {Critical | Private | Warning}
 set match-percentage <integer>
 set action {allow | log-only | block | ban | quarantine-ip}
 next
 end
 next
end

```

Command	Description
<code>proto {smtp   pop3   imap http-get   http-post   ftp   nntp   mapi}</code>	The protocol to inspect.
<code>filter-by fingerprint</code>	Match against a fingerprint sensitivity.
<code>sensitivity {Critical   Private   Warning}</code>	Select a DLP file pattern sensitivity to match.
<code>match-percentage &lt;integer&gt;</code>	The percentage of the checksum required to match before the sensor is triggered.
<code>action {allow   log-only   block   ban   quarantine-ip}</code>	The action to take with content that this DLP sensor matches.

### View the DLP fingerprint database on the FortiGate

The CLI debug command `diagnose test application dlpfingerprint` can be used to display the fingerprint information that is on the FortiGate.

```

Fingerprint Daemon Test Usage;

1 : This menu
2 : Dump database
3 : Dump all files
5 : Dump all chunk
6 : Refresh all doc sources in all VDOMs
7 : Show the db file size and the limit
9 : Display stats

```

```
10 : Clear stats
99 : Restart this daemon
```

For example, option 3 will dump all fingerprinted files:

```
DLP_WANOPT-CLT (global) # diagnose test application dlpfingerprint 3
```

```
DLPFP diag_test_handler called
```

```
File DB:
```

```

id, filename, vdom, archive, deleted, scanTime, docSourceSrvr,
sensitivity, chunkCnt, reviseCnt,
1, /fingerprint/upload/1.txt, vdom1, 0, 0, 1494868196, 1, 2,
1, 0,
2, /fingerprint/upload/30percentage.xls, vdom1, 0, 0, 1356118250, 1, 2,
13, 0,
3, /fingerprint/upload/50.pdf, vdom1, 0, 0, 1356118250, 1, 2,
122, 0,
4, /fingerprint/upload/50.pdf.tar.gz, vdom1, 0, 0, 1356118250, 1, 2,
114, 0,
5, /fingerprint/upload/check-list_AL-SIP_HA.xls, vdom1, 0, 0, 1356118251, 1,
2, 32, 0,
6, /fingerprint/upload/clean.zip, vdom1, 0, 0, 1356118251, 1, 2,
1, 0,
7, /fingerprint/upload/compare.doc, vdom1, 0, 0, 1522097410, 1, 2,
18, 0,
8, /fingerprint/upload/dlpsensor-watermark.pdf, vdom1, 0, 0, 1356118250, 1,
2, 11, 0,
9, /fingerprint/upload/eicar.com, vdom1, 0, 0, 1356118250, 1, 2,
1, 0,
10, /fingerprint/upload/eicar.zip, vdom1, 0, 0, 1356118250, 1, 2,
1, 0,
11, /fingerprint/upload/EMAIL-CONTENT-ARCHIVE.ppt, vdom1, 0, 0, 1356118250, 1,
2, 11, 0,
12, /fingerprint/upload/encrypt.zip, vdom1, 0, 0, 1356118250, 1, 2,
77, 0,
13, /fingerprint/upload/extension_7_8_1.crx, vdom1, 0, 0, 1528751781, 1,
2, 2720, 0,
14, /fingerprint/upload/fingerprint.txt, vdom1, 0, 0, 1498582679, 1, 2,
37, 0,
15, /fingerprint/upload/fingerprint90.txt, vdom1, 0, 0, 1498582679, 1, 2,
37, 0,
16, /fingerprint/upload/fo2.pdf, vdom1, 0, 0, 1450488049, 1, 2,
1, 0,
17, /fingerprint/upload/foo.doc, vdom1, 0, 0, 1388538131, 1, 2,
9, 0,
18, /fingerprint/upload/fortiauto.pdf, vdom1, 0, 0, 1356118251, 1, 2,
146, 0,
19, /fingerprint/upload/image.out, vdom1, 0, 0, 1531802940, 1, 2,
5410, 0,
20, /fingerprint/upload/jon_file.txt, vdom1, 0, 0, 1536596091, 1, 2, 1,
0,
21, /fingerprint/upload/machotest, vdom1, 0, 0, 1528751955, 1, 2,
19, 0,
22, /fingerprint/upload/nntp-server.doc, vdom1, 0, 0, 1356118250, 1, 2,
17, 0,
23, /fingerprint/upload/notepad++.exe, vdom1, 0, 0, 1456090734, 1, 2,
1061, 0,
24, /fingerprint/upload/nppIExplorerShell.exe, vdom1, 0, 0, 1438559930, 1,
2, 5, 0,
25, /fingerprint/upload/NppShell_06.dll, vdom1, 0, 0, 1456090736, 1, 2,
111, 0,
```

```

26, /fingerprint/upload/PowerCollections.chm, vdom1, 0, 0, 1533336889, 1,
2, 728, 0,
27, /fingerprint/upload/reflector.dmg, vdom1, 0, 0, 1533336857, 1, 2,
21117, 0,
28, /fingerprint/upload/roxio.iso, vdom1, 0, 0, 1517531765, 1, 2,
49251,0,
29, /fingerprint/upload/SciLexer.dll, vdom1, 0, 0, 1456090736, 1, 2,
541, 0,
30, /fingerprint/upload/screen.jpg, vdom1, 0, 0, 1356118250, 1, 2,
55, 0,
31, /fingerprint/upload/Spec to integrate FASE into FortiOS.doc, vdom1, 0, 0,
1356118251, 1, 2, 31, 0,
32, /fingerprint/upload/subdirectory1/subdirectory2/subdirectory3/hibun.aea, vdom1, 0,
0, 1529019743, 1, 2, 1, 0,
33, /fingerprint/upload/test.pdf, vdom1, 0, 0, 1356118250, 1, 2,
5, 0,
34, /fingerprint/upload/test.tar, vdom1, 0, 0, 1356118251, 1, 2,
3, 0,
35, /fingerprint/upload/test.tar.gz, vdom1, 0, 0, 1356118250, 1, 2, 1,
0,
36, /fingerprint/upload/test1.txt, vdom1, 0, 0, 1540317547, 1, 2,
1, 0,
37, /fingerprint/upload/thousand-files.zip, vdom1, 0, 0, 1536611774, 1, 2,
241, 0,
38, /fingerprint/upload/Thumbs.db, vdom1, 0, 0, 1445878135, 1, 2,
3, 0,
39, /fingerprint/upload/widget.pdf, vdom1, 0, 0, 1356118251, 1, 2,
18, 0,
40, /fingerprint/upload/xx00-xx01.tar, vdom1, 0, 0, 1356118250, 1, 2, 5,
0,
41, /fingerprint/upload/xx02-xx03.tar.gz, vdom1, 0, 0, 1356118251, 1, 2, 1,
0,

```

## VoIP solutions

You can configure VoIP profiles to allow SIP and SCCP traffic and to protect your network from SIP- and SCCP-based attacks.

FortiOS includes two preloaded VoIP profiles:

- *default*
- *strict*

You can customize these profiles, or you can create your own and add them to firewall policies that allow VoIP.

The following topics provide information about VoIP profiles:

- [General use cases on page 1067](#)
- [SIP message inspection and filtering on page 1070](#)
- [SIP pinholes on page 1072](#)
- [SIP over TLS on page 1073](#)
- [Custom SIP RTP port range support on page 1074](#)
- [Voice VLAN auto-assignment on page 1075](#)



## General use cases

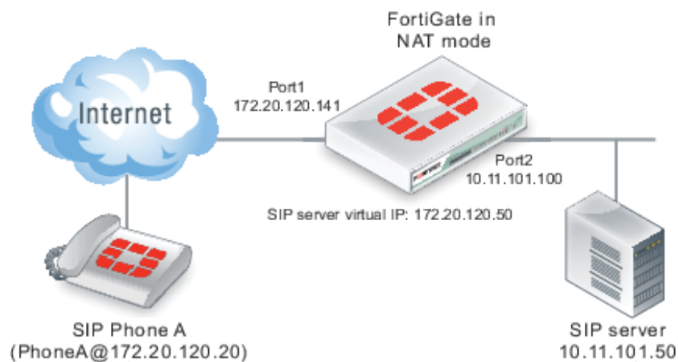
There are three scenarios in which the FortiOS session initiation protocol (SIP) solution is usually deployed:

1. The SIP server is in a private network, protected from the internet by a FortiOS device.
2. The SIP clients are in a private network, protected from the internet by a FortiOS device.
3. The SIP server is in a private network, such as a corporation's internal network or an ISP's network, protected from the Internet by a FortiOS device. The SIP clients are in a remote private network, such as a SOHO network, and behind a NAT device that is not aware of SIP applications.

The following VIP, NAT, and HNT examples show configurations for each of the three common scenarios.

### VIP

A FortiGate with SIP Application Layer Gateway (ALG) or SIP Session Helper protects the SIP server from the internet, while SIP phones from the internet need to register to the SIP server and establish calls through it.



A VIP needs to be configured for the SIP server, and the VIP must be applied in a firewall policy for the phones to send REGISTER messages through the FortiGate from port1 to port2.

Only one firewall policy needs to be configured for all SIP phones on both the internet and private network to register to the SIP server through Port1 and set up SIP calls.

Assuming either SIP ALG or SIP Session Helper is enabled, configure the FortiGate with the following CLI commands:

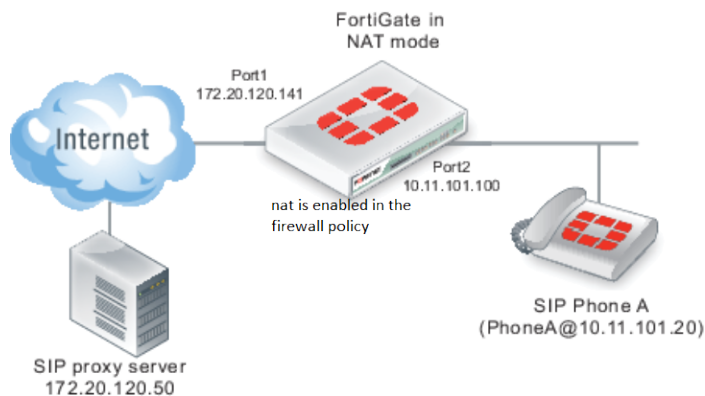
```
config firewall vip
 edit "VIP_for_SIP_Server"
 set extip 172.20.120.50
 set extintf "port1"
 set mappedip "10.11.101.50"
 next
end
config firewall policy
 edit 1
 set srcintf "port1"
 set dstintf "port2"
 set srcaddr "all"
 set dstaddr "VIP_for_SIP_Server"
 set action accept
 set schedule "always"
 set service "SIP"
 next
end
```



Setting `service` to `SIP` and not `All` in the firewall policy can improve protection by restricting the data traffic passing through the FortiGate to the SIP call traffic only.

## NAT

A FortiGate with SIP ALG or SIP Session Helper protects the SIP phones and the internal network from the internet, while SIP phones in the internal network need to register to the SIP server installed on the internet and establish calls through it.



One firewall policy needs to be configured with NAT enabled for SIP phones to send REGISTER messages through the FortiGate from port2 to port1.

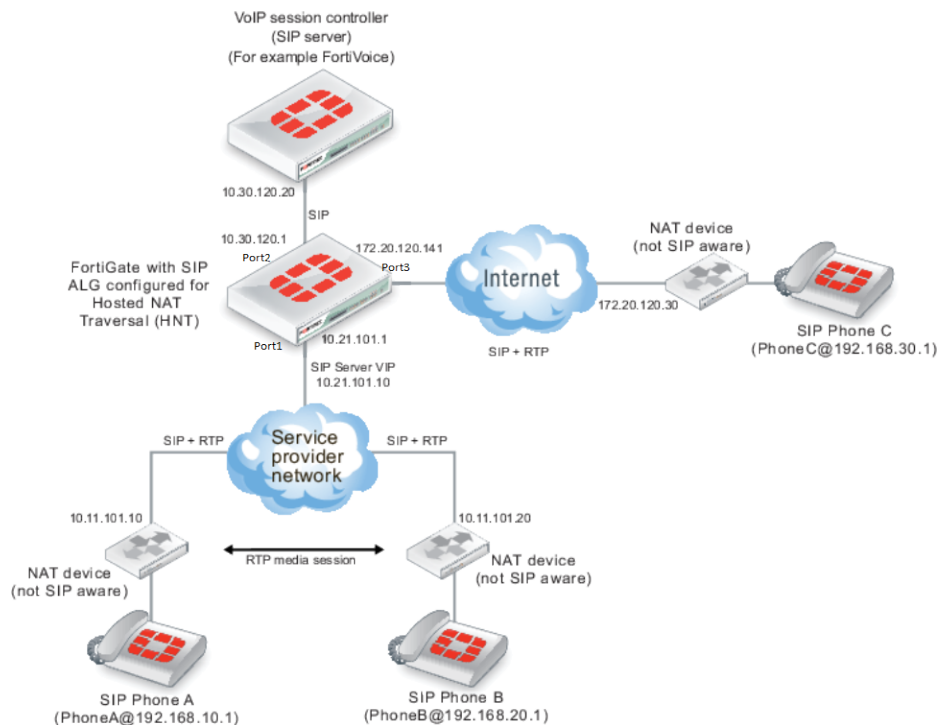
Assuming either SIP ALG or SIP Session Helper is enabled, configure the FortiGate with the following CLI commands:

```
config firewall policy
 edit 1
 set srcintf "port2"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "SIP"
 set nat enable
 next
end
```

## HNT

A FortiGate with SIP ALG or SIP Session Helper protects the SIP server from the internet, while SIP phones are in remote private networks behind NAT devices that are not aware of the SIP application.

For example, the SIP server is located in an ISP's service cloud that is protected by the FortiGate SIP ALG, and the SIP phones are installed in the home networks of the ISP's customers.



The SIP messages traversing the remote NAT devices might have their IP addresses translated by the NAT device at the network layer, but untranslated at the SIP application layer because those NAT devices are not aware of the SIP applications. This causes problems in a SIP session initiated process. Special configurations for the Hosted NAT Traversal (HNT) are required to resolve this issue.

**To configure the FortiGate with HNT support for SIP phones A and B to set up calls with each other:**

1. Identify port1 as the external interface:

```
config system interface
 edit "port1"
 set external enable
 next
end
```

2. Configure VIP for the SIP server:

```
config firewall vip
 edit "VIP_for_SIP_Server"
 set extip 10.21.101.10
 set extintf "port1"
 set mappedip "10.30.120.20"
 next
end
```

3. Configure a VoIP profile with HNT enabled:

```
config voip profile
 edit "hnt"
 config sip
 set hosted-nat-traversal enable
 set hnt-restrict-source-ip enable
 end
 end
```

```
 end
 next
end
```



hosted-nat-traversal must be enabled.

hnt-restrict-source-ip does not have to be enabled, but can be enabled to restrict the RTP packets' source IP to be the same as the SIP packets' source IP.

- 
4. Apply the VoIP profile and VIP in a firewall policy for phone A and B to register and set up SIP calls through the FortiGate and SIP server:

```
config firewall policy
 edit 1
 set srcintf "port1"
 set dstintf "port2"
 set srcaddr "all"
 set dstaddr "VIP_for_SIP_Server"
 set action accept
 set schedule "always"
 set service "SIP"
 set utm-status enable
 set voip-profile "hnt"
 set nat enable
 next
end
```



nat must be enabled in the firewall policy.

---

## SIP message inspection and filtering

SIP ALG provides users with security features to inspect and control SIP messages that are transported through FortiOS devices, including:

- Verifying the SIP message syntax.
- Blocking particular types of SIP requests.
- Restricting the rate of particular SIP requests.

These features are configured in the VoIP profile:

```
config voip profile
 edit <voip_profile_name>
 config sip set ...
```

The VoIP profile can then be applied to a firewall policy to process the SIP call traffic.

### SIP message syntax inspection

For syntax verification, the following attributes are available for configuration in the VoIP profile to determine what action is taken when a specific syntax error or attack based on invalid syntax is detected. For example, the action can be set to pass or discard it.

- malformed-request-line
- malformed-header-via
- malformed-header-from
- malformed-header-to
- malformed-header-call-id
- malformed-header-cseq
- malformed-header-rack
- malformed-header-rseq
- malformed-header-contact
- malformed-header-record-route
- malformed-header-route
- malformed-header-expires
- malformed-header-content-type
- malformed-header-content-length
- malformed-header-max-forwards
- malformed-header-allow
- malformed-header-p-asserted-identity
- malformed-header-sdp-v
- malformed-header-sdp-o
- malformed-header-sdp-s
- malformed-header-sdp-i
- malformed-header-sdp-c
- malformed-header-sdp-b
- malformed-header-sdp-z
- malformed-header-sdp-k
- malformed-header-sdp-a
- malformed-header-sdp-t
- malformed-header-sdp-r
- malformed-header-sdp-m

### SIP message blocking

The following options are available in the VoIP profile to block SIP messages:

- block-long-lines
- block-unknown
- block-ack
- block-bye
- block-cancel
- block-info
- block-invite
- block-message
- block-notify
- block-options
- block-prack
- block-publish
- block-refer
- block-register
- block-subscribe
- block-update
- block-geo-red-options

### SIP message rate limiting

The rate of certain types of SIP requests that are passing through the SIP ALG can be restricted :

```
register-rate
invite-rate
subscribe-rate
message-rate
notify-rate
refer-rate
update-rate
options-rate
ack-rate
prack-rate
info-rate
publish-rate
bye-rate
cancel-rate
```

## SIP pinholes

When SIP ALG processes a SIP call, it usually opens pinholes for SIP signaling and RTP/RTCP packets. NAT usually takes place during the process at both the network and SIP application layers. SIP ALG ensures that, with NAT happening, corresponding SIP and RTP/RTCP pinholes are created during the process when it is necessary for call sessions to be established through FortiOS devices.

By default, SIP ALG manages pinholes automatically, but some special configurations can be used to restrict the pinholes if required.

### SIP pinhole restriction

By default, the *strict-register* attribute is enabled. When enabled, after a SIP endpoint registers to the SIP server through a firewall policy on the FortiOS device, only the SIP messages sent from the same IP address as the SIP server are allowed to pass through the SIP pinhole that is created in the FortiOS device to reach the SIP endpoints. If the attribute is disabled, SIP messages from any IP addresses can pass through the pinhole created after the registration.

```
config voip profile
 edit "voip-profile-name"
 config sip
 set strict-register [enable|disable]
 ...
 end
 next
end
```

### RTP/RTCP pinhole restriction

In a SIP call through SIP ALG, the NATed RTP/RTCP port range is 5117 to 65533 by default. If required, the port range can be restricted.

```
config voip profile
 edit "voip-profile-name"
 config sip
 set nat-port-range <start_port_number>-<end_port_number>
 ...
 end
```

```
 next
end
```

In a SIP call session, the RTP port number is usually an even number and the RTCP port number is an odd number that is one more than the RTP port number. It is best practice to configure `start_port_number` to an even number, and `end_port_number` to an odd number, for example:

```
config voip profile
 edit "voip-profile-name"
 conf sip
 set nat-port-range 30000-39999
 end
 next
end
```

## SIP over TLS

Some SIP phones and servers can communicate using TLS to encrypt the SIP signaling traffic. To allow SIP over TLS calls to pass through the FortiGate, the encrypted signaling traffic must be unencrypted and inspected. The FortiGate SIP ALG intercepts, unencrypts, and inspects the SIP packets, which are then re-encrypted and forwarded to their destination.

The SIP ALG only supports full mode TLS. This means that the SIP traffic between SIP phones and the FortiGate, and between the FortiGate and the SIP server, is always encrypted. The highest TLS version supported by SIP ALG is TLS 1.2.

To enable SIP over TLS support, the SSL mode in the VoIP profile must be set to `full`. The SSL server and client certificates can be provisioned so that the FortiGate can use them to establish connections to SIP phones and servers, respectively.

### To configure SIP over TLS:

1. Configure a VoIP profile with SSL enabled:

```
config voip profile
 edit "tls"
 config sip
 set ssl-mode full
 set ssl-client-certificate "ssl_client_cert"
 set ssl-server-certificate "ssl_server_cert"
 end
 next
end
```

The `ssl_server_cert`, `ssl_client_cert`, and key files can be generated using a certification tool, such as OpenSSL, and imported to the local certificate store of the FortiGate from *System > Certificates* in the GUI. Existing local certificates in the certificate store can also be used. As always for TLS connections, the certificates used must be verified and trusted at the other end of the connection when required.

For example, the CA certificate of the SIP server's certificate should be imported to the FortiGate as an external CA certification, such that the FortiGate can use it to verify the SIP server's certificate when setting up the TLS connection. The CA certificate configured as the `ssl_server_cert` should be installed as the trusted certificate on the SIP phones. The deployment of the certificates across the network depends on the SIP client and server devices that are used in the system.

**2. Apply the profile to the firewall policy:**

```
config firewall policy
 edit 1
 set srcintf "port1"
 set dstintf "port2"
 set srcaddr "all"
 set dstaddr "vip_sip_server"
 set action accept
 set schedule "always"
 set service "SIP"
 set utm-status enable
 set voip-profile "tls"
 next
end
```

## Custom SIP RTP port range support

The `nat-port-range` variable is used to specify a port range in the VoIP profile to restrict the NAT port range for real-time transport protocol/real-time transport control protocol (RTP/RTCP) packets in a session initiation protocol (SIP) call session that is handled by the SIP application layer gateway (ALG) in a FortiGate device.

When NAT is enabled, or VIP is used in a firewall policy for SIP ALG to handle a SIP call session established through a FortiGate device, the SIP ALG can perform NAT to translate the ports used for the RTP/RTCP packets when they are flowing through the device between the external and internal networks.

You can control the translated port range for RTP/RTCP packets using the CLI:

```
config voip profile
 edit <profile-name>
 config sip
 set nat-port-range <port range>
 end
 next
end
```

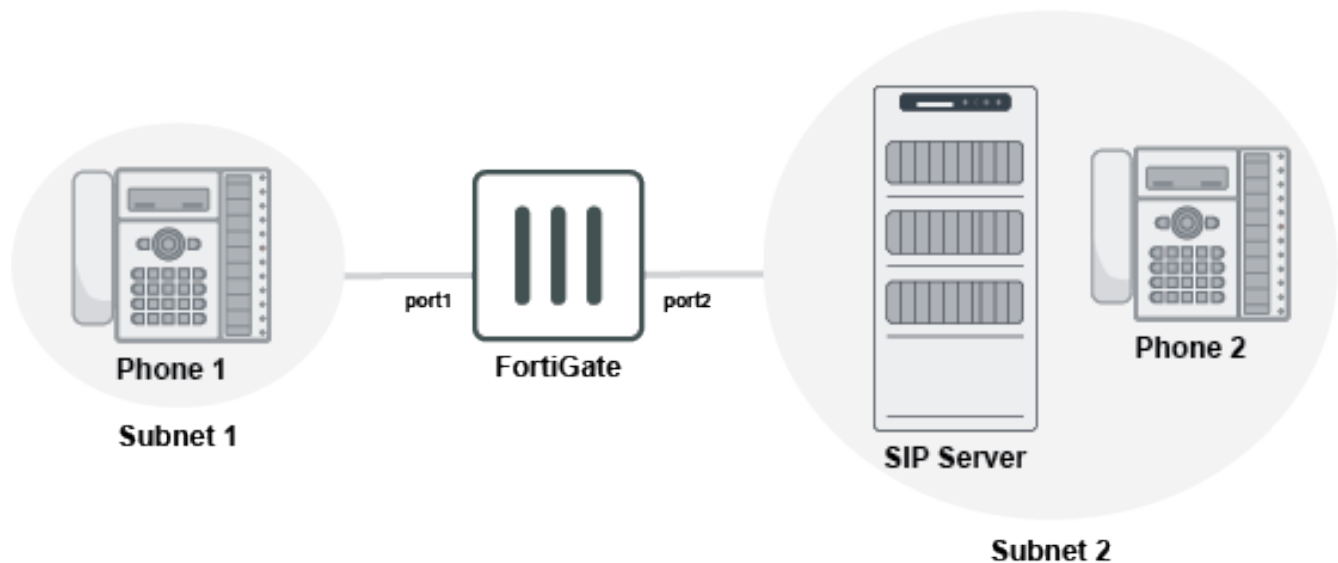
Command	Description
<code>nat-port-range &lt;port range&gt;</code>	The NAT port range (minimum port number = 5117, default = 5117-65535).

### Example

In this example, Phone1 is in subnet\_1, and the SIP server and phone are in subnet\_2. All SIP signaling messages and RTP/RTCP packets go through the SIP Server. The RTP/RTCP ports on Phone1 are configured as 17078/17079.

The FortiGate administrator wants to use NAT for the port 17078/17079 to 30000/30001. As a result, all RTP/RTCP packets going out of port2 have source ports of 30000/30001, and all RTP/RTCP packets going into port2 also have destination ports of 30000/30001, which is specified in `nat-port-range`.





### To configure the custom port range:

```
config voip profile
 edit "natPortRange"
 config sip
 set nat-port-range 30000-30001
 end
 next
end
configure firewall policy
 edit 1
 set srcintf port1
 set dstintf port2
 set srcaddr all
 set dstaddr all
 set service SIP
 set action accept
 set schedule always
 set voip-profile natPortRange
 set nat enable
 end
end
```

If phone1 and phone2 are registered to the SIP server, and they establish a call session between them through the FortiGate and the SIP server, then the RTP/RTCP ports 17078/17079 of phone1 will be translated to ports 30000/30001 at the FortiGate unit based on the NAT port range setting. That is, the RTP/RTCP packets egressing port2 of the Fortigate will have source ports of 30000/30001, and the RTP/RTCP packets ingressing port2 will have destination ports of 30000/30001.

## Voice VLAN auto-assignment

You can leverage LLDP-MED to assign voice traffic to the desired voice VLAN. After detection and setup, the IP phone on the network is segmented to its own VLAN for policy, prioritization, and reporting. The LLDP reception capabilities in FortiOS have been extended to support LLDP-MED assignment for voice, voice signaling, guest, guest voice signaling, softphone, video conferencing, streaming video, and video signaling.

You can configure this feature using the following steps:

1. [Setting up the VLAN for the voice device](#)
2. [Setting up the DHCP server for the voice VLAN](#)
3. [Setting up the LLDP network policy](#)
4. [Enabling LLDP on the physical interface that the VLAN belongs to](#)
5. [Applying the LLDP network policy on the physical interface](#)
6. [Confirming that the VLAN was assigned](#)

**To set up the VLAN for the voice device:**

```
config system interface
 edit "vlan_100"
 set vdom "root"
 set ip 192.168.1.99 255.255.255.0
 set alias "voice_vlan"
 set device-identification enable
 set role lan
 set snmp-index 25
 set interface "port10"
 set vlanid 100
 next
end
```

**To set up the DHCP server for the voice VLAN:**

```
config system dhcp server
 edit 1
 set dns-service default
 set default-gateway 192.168.1.99
 set netmask 255.255.255.0
 set interface "vlan_100"
 config ip-range
 edit 1
 set start-ip 192.168.1.110
 set end-ip 192.168.1.210
 next
 end
 next
end
```

**To set up the LLDP network policy:**

```
config system lldp network-policy
 edit "1"
 config voice
 set status enable
 set tag dot1q
 set vlan 100
 end
 next
end
```

**To enable LLDP on the physical interface that the VLAN belongs to:**

```
config system interface
 edit "port10"
 set vdom "root"
 set type physical
 set lldp-reception enable
 set lldp-transmission enable
 set snmp-index 14
 next
end
```

**To apply the LLDP network policy on the physical interface:**

```
config system interface
 edit "port10"
 set lldp-network-policy "1"
 next
end
```

**To confirm that the VLAN was assigned as expected:**

1. Connect an IP phone to the network.
2. Check the IP address on the phone.  
The IP address should belong to the voice VLAN.
3. Sniff on the FortiGate incoming interface to see if traffic from the IP phone has the desired VLAN tag.  
In the example commands above, the voice VLAN was configured as VLAN 100. Therefore, voice traffic from the IP phone should be in VLAN 100.

## ICAP

Internet Content Adaptation Protocol (ICAP) is an application layer protocol that is used to offload tasks from the firewall to separate, specialized servers. For more information see [RFC 3507](#).

ICAP profiles can only be applied to policies that use proxy-based inspection. If you enable ICAP in a policy, HTTP and HTTPS (if HTTPS inspection is supported) traffic that is intercepted by the policy is transferred to the ICAP server specified by the selected ICAP profile. Responses from the ICAP server are returned to the FortiGate, and then forwarded to their destination.



By default, *ICAP* is not visible in the GUI. See [Feature visibility on page 732](#) for instructions on making it visible.

---

**To configure ICAP:**

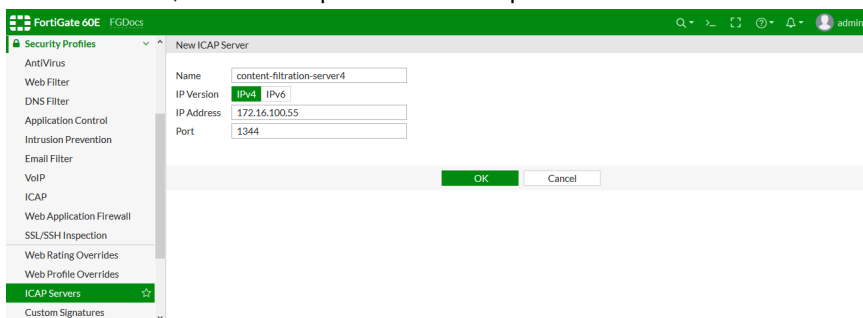
1. Set up your ICAP server.
2. On the FortiGate, add an ICAP server.
3. Create an ICAP profile.
4. Use the ICAP profile in a firewall policy that covers the traffic that needs to be offloaded to the ICAP server.

## ICAP configuration example

In this example, the ICAP server performs proprietary content filtering on HTTP and HTTPS requests. If the content filter is unable to process a request, then the request is blocked. Streaming media is not considered by the filter, so it is allowed through and is not processed.

### To add the ICAP server to the FortiGate in the GUI:

1. Go to *Security Profiles > ICAP Servers*.
2. Click *Create New*.
3. In the *Name* field, enter a name for the ICAP server, such as *content-filtration-server4*.
4. Select the *IP Version*.
5. In the *IP Address* field, enter the IP address of the ICAP server.
6. In the *Port* field, enter a new port number if required. The default value is *1344*.



7. Click *OK*.

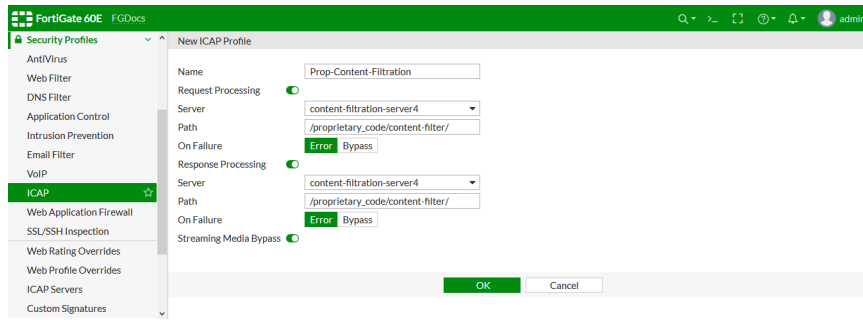


The maximum number of concurrent connections to ICAP server can be configured in the CLI. The default setting is 100 connections.

### To create an ICAP profile in the GUI:

1. Go to *Security Profiles > ICAP*.
2. Click *Create New*.
3. In the *Name* field, enter a name for the ICAP profile, such as *Prop-Content-Filtration*.
4. Enable *Request Processing* then set the following:
  - *Server* - Select the ICAP server. In this example, select *content-filtration-server4*
  - *Path* - The path to the processing component on the server, such as */proprietary\_code/content-filter/*.
  - *On Failure* - Select *Error* to block the request. If the message cannot be processed, it will not be blocked.
5. Enable *Response Processing* then set the following:
  - *Server* - Select the ICAP server: *content-filtration-server4*
  - *Path* - The path to the processing component on the server, such as */proprietary\_code/content-filter/*.
  - *On Failure* - Select *Error* to block the request. If the message cannot be processed, it will not be blocked.

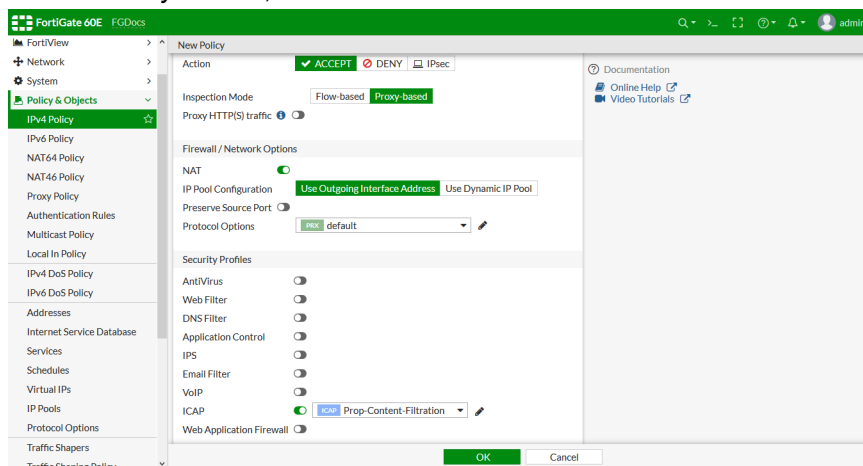
6. Enable *Streaming Media Bypass* to not offload streaming media to the ICAP server.



7. Click **OK**.

**To add the ICAP profile to a policy in the GUI:**

1. Go to *Policy & Objects > IPv4 Policy*.
2. Click *Create New*.
3. Configure the policy as needed to apply to the required traffic.
4. Set *Inspection Mode* to *Proxy-based*.
5. Under *Security Profiles*, enable *ICAP* and select the ICAP server.



6. Click **OK**.

**To configure the ICAP setup in the CLI:**

1. Add the ICAP server:

```
config icap server
 edit "content-filtration-server4"
 set ip-version 4
 set ip-address 172.16.100.55
 set port 1344
 set max-connections 200
 next
end
```

**2. Create the ICAP profile:**

```
config icap profile
 edit "Prop-Content-Filtration"
 set request enable
 set response enable
 set streaming-content-bypass enable
 set request-server "content-filtration-server4"
 set response-server "content-filtration-server4"
 set request-failure error
 set response-failure error
 set request-path "/proprietary_code/content-filter/"
 set response-path "/proprietary_code/content-filter/"
 set methods delete get head options post put trace other
 next
end
```

**3. Add the ICAP profile to a policy:**

```
config firewall policy
 edit 5
 set name "icap_filter3"
 set srcintf "virtual-wan-link"
 set dstintf "virtual-wan-link"
 set srcaddr "FABRIC_DEVICE"
 set dstaddr "FABRIC_DEVICE"
 set dstaddr-negate enable
 set action accept
 set schedule "always"
 set service "ALL"
 set utm-status enable
 set inspection-mode proxy
 set ssl-ssh-profile "certificate-inspection"
 set icap-profile "Prop-Content-Filtration"
 set logtraffic disable
 set fsso disable
 set nat enable
 next
end
```

## Web application firewall

Web application firewall (WAF) profiles can detect and block known web application attacks. You can configure WAF profiles to use signatures and constraints to examine web traffic. You can also enforce an HTTP method policy, which controls the HTTP method that matches the specified pattern.

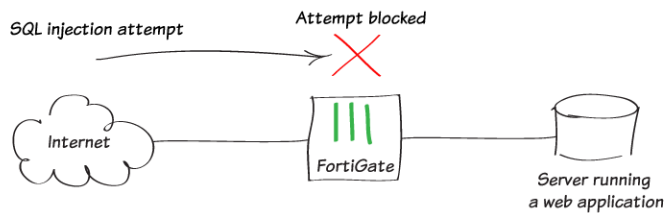
You can customize the default profile, or you can create your own profile to apply access rules and HTTP protocol constraints to traffic. You can apply WAF profiles to firewall policies when the inspection mode is set to proxy-based.

The following topic provides information about WAF profiles:

- [Protecting a server running web applications on page 1081](#)

## Protecting a server running web applications

You can use a web application firewall profile to protect a server that is running a web application, such as webmail.



Web application firewall profiles are created with a variety of options called signatures and constraints. Once these options are enabled, the action can be set to allow, monitor, or block. The severity can be set to high, medium, or low.

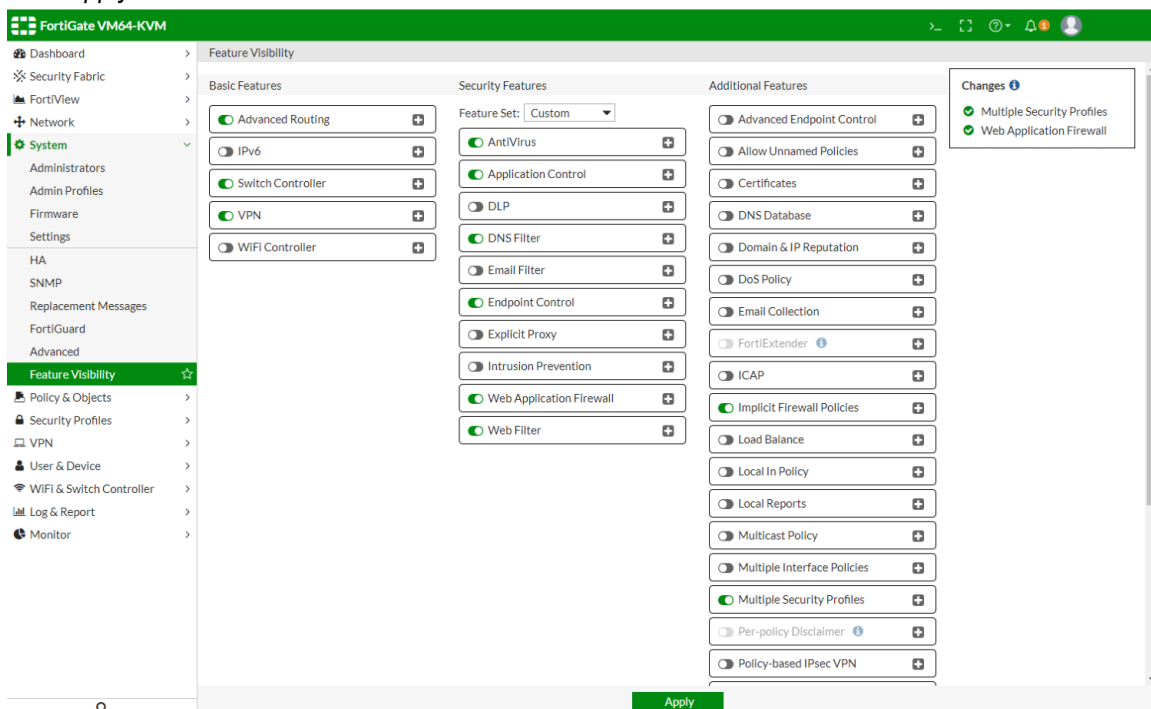
In the following example, the default profile will be targeted to block SQL injection attempts and generic attacks.



The web application firewall feature is only available when the policy inspection mode is proxy-based.

### To protect a server running web applications:

1. Enable the web application firewall:
  - a. Go to *System > Feature Visibility*.
  - b. Under *Security Features*, enable *Web Application Firewall*.
  - c. Under *Additional Features*, click *Show More* and enable *Multiple Security Profiles*.
  - d. Click *Apply*.



2. Edit the default web application firewall profile:  
*Trojans and Known Exploits are blocked by default.*
  - a. Go to *Security Profiles > Web Application Firewall*.
  - b. Edit the *default* profile signature:
    - i. Enable *SQL Injection (Extended)* and *Generic Attacks (Extended)*.
    - ii. For both signatures, set the *Action* to *Block* and the *Severity* to *High*.
  - iii. Click *Apply*.

**Signatures**

Enable	Signature	Action	Severity
<input type="checkbox"/>	Cross Site Scripting	Monitor	Medium
<input type="checkbox"/>	Cross Site Scripting (Extended)	Monitor	Medium
<input checked="" type="checkbox"/>	SQL Injection	Block	High
<input checked="" type="checkbox"/>	SQL Injection (Extended)	Block	High
<input checked="" type="checkbox"/>	Generic Attacks	Block	High
<input checked="" type="checkbox"/>	Generic Attacks(Extended)	Block	High
<input checked="" type="checkbox"/>	Trojans	Block	High
<input checked="" type="checkbox"/>	Information Disclosure	Monitor	Low
<input checked="" type="checkbox"/>	Known Exploits	Block	High
<input type="checkbox"/>	Credit Card Detection	Block	High
<input checked="" type="checkbox"/>	Bad Robot	Monitor	High

**Constraints**

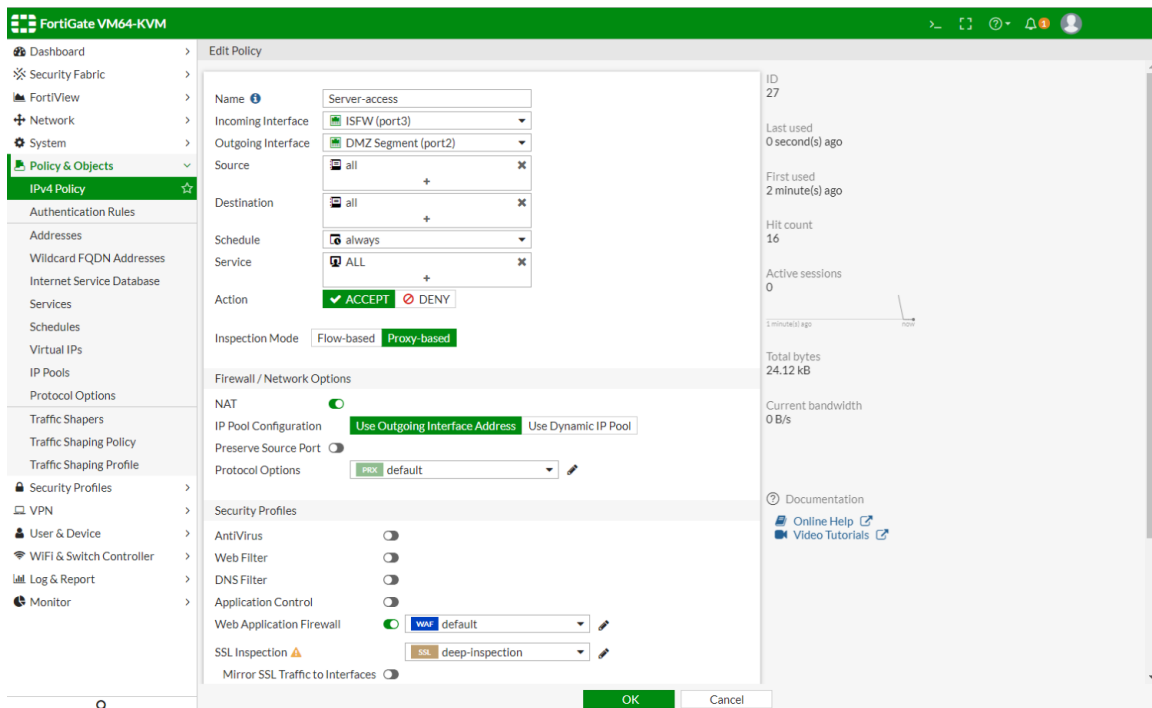
Enable	Constraint	Limit	Action	Severity
<input type="checkbox"/>	Illegal Host Name	-	Block	Medium
<input type="checkbox"/>	Illegal HTTP Version	-	Monitor	Medium
<input type="checkbox"/>	Illegal HTTP Request Method	-	Block	Medium
<input checked="" type="checkbox"/>	Content Length	67108864	Monitor	Low
<input checked="" type="checkbox"/>	Header Length	8192	Monitor	Low
<input checked="" type="checkbox"/>	Header Line Length	1024	Monitor	Low
<input checked="" type="checkbox"/>	Number of Header Lines in Request	32	Monitor	Low
<input checked="" type="checkbox"/>	Total URL and Body Parameters Length	8192	Monitor	Low
<input checked="" type="checkbox"/>	Total URL Parameters Length	8192	Monitor	Low
<input checked="" type="checkbox"/>	Number of URL Parameters	16	Monitor	Low
<input checked="" type="checkbox"/>	Number of Cookies in Request	16	Monitor	Low
<input checked="" type="checkbox"/>	Number of Ranges in Range Header	5	Monitor	High
<input type="checkbox"/>	Malformed Request	-	Monitor	Medium

**Apply**

3. Apply the profile to a security policy:
  - a. Go to *Policy & Objects > IPv4 Policy*.
  - b. Edit the policy that allows access to the web server:
    - i. Under *Firewall / Network Options*, select the appropriate *Protocol Option*.
    - ii. Under *Security Profiles*, enable *Web Application Firewall* and set it to use the *default* profile.
    - iii. Set the *SSL Inspection* to use the *deep-inspection* profile.



## iv. Click OK.



## 4. Verify that the web application firewall blocks traffic:

- a. Use the following URL to simulate an attack on your web server and substitute the IP address of your server:

`http://<server`

`IP>/index.php?username=1'%20or%20'1'%20=%20'1&password=1'%20or%20'1'%20=%20'1`

An error message appears, stating that the web application firewall has blocked the traffic:



## Offloading to a FortiWeb

If you have a FortiWeb, you may be able to offload the functions of the web application control to your FortiWeb. To find out if this option is available, refer to the FortiOS or FortiWeb Release Notes for information about device compatibility.

### To offload to a FortiWeb:

1. Go to *Security Fabric > Settings*.
2. Enable *Fabric Devices*.
3. Enter the following for the device:
  - a. Name (FortiWeb)
  - b. FortiWeb IP address

## c. HTTPS service port

FortiGate 900D FortiGate-900D

Dashboard > Security Fabric Settings

Security Fabric >

Physical Topology

Logical Topology

Security Rating

Automation

Settings ☆

Fabric Connectors

FortiView >

Network >

System >

Policy & Objects >

Security Profiles >

VPN >

User & Device >

WiFi & Switch Controller >

Log & Report >

Monitor >

FortiGate Telemetry

FortiAnalyzer Logging

Central Management

Type FortiManager FortiManager Cloud **FortiGate Cloud**

Account **Activate**

Sandbox Inspection

Fabric Devices

Name

IP 0.0.0.0

HTTPS port 443

Access token **Generate**

Token test results ? **Test**

4. Click **Generate**.
5. Enter your credentials to generate the access token.
6. Click **OK**.

## Inspection modes

This section contains the following topics:

- [About inspection modes on page 1084](#)
- [SSL Inspection on page 1091](#)
- [SSH traffic file scanning on page 1098](#)

### About inspection modes

FortiOS supports flow-based and proxy-based inspection in firewall policies. You can select the inspection mode when configuring a policy.

Flow-based inspection takes a snapshot of content packets and uses pattern matching to identify security threats in the content.

Proxy-based inspection reconstructs content that passes through the FortiGate and inspects the content for security threats.

Each inspection mode plays a role in processing traffic en route to its destination. While both modes offer significant security, proxy-based provides more feature configuration options, while flow-based is designed to optimize performance.

The following topics provide information about inspection modes for various security profile features:

- [Flow mode inspection \(default mode\) on page 1085](#)
- [Proxy mode inspection on page 1086](#)
- [Inspection mode feature comparison on page 1087](#)
- [Inspection mode differences for antivirus on page 1088](#)
- [Inspection mode differences for data leak prevention on page 1089](#)
- [Inspection mode differences for email filter on page 1090](#)
- [Inspection mode differences for web filter on page 1091](#)

## Flow mode inspection (default mode)

When a firewall policy's inspection mode is set to *flow*, traffic flowing through the policy will not be buffered by the FortiGate. Unlike proxy mode, the content payload passing through the policy will be inspected on a packet by packet basis with the very last packet held by the FortiGate until the scan returns a verdict. If a violation is detected in the traffic, a reset packet is issued to the receiver, which terminates the connection, and prevents the payload from being sent successfully.

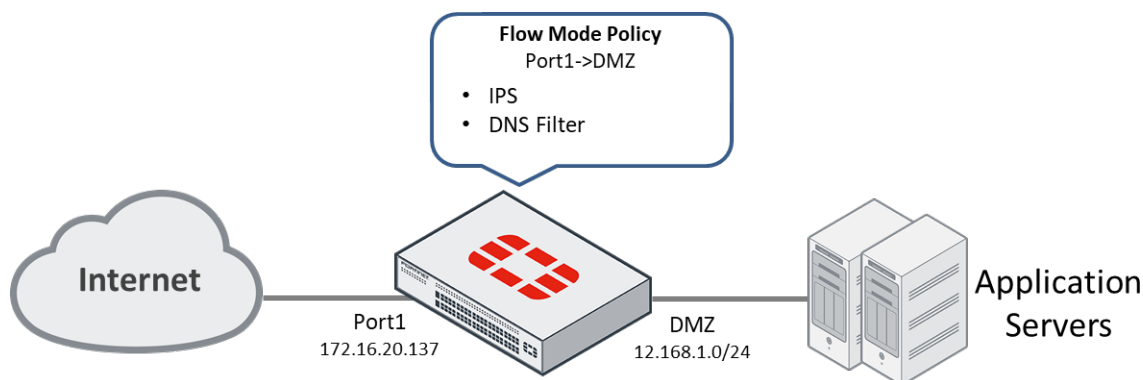
Because of this method, flow mode inspection cannot be as thorough as proxy mode inspection and will have some feature limitations. For example, flow mode inspection determines a file's size by identifying the file size information in the protocol exchange. If a file's size is not present in the protocol exchange, the file's size cannot be identified. The flow-based policy will automatically block or pass the file (based on the configuration) despite the file meeting the file size requirements.

The objective of flow-based policy is to optimize performance and increase throughput. Although it is not as thorough as a proxy-based policy, flow mode inspection is still very reliable.

## Use case

It is recommended that flow inspection is applied to policies that prioritize traffic throughput, such as allowing connections to be made towards a streaming or file server.

You have an application server which accepts connections from users for the daily quiz show app, HQ. Each HQ session sees 500,000+ participants, and speed is very important because participants have less than 10 seconds to answer the quiz show questions.



In this scenario, a flow inspection policy is recommended to prioritize throughput. The success of the application depends on providing reliable service for large numbers of concurrent users. We will apply an IPS sensor to this policy to protect the server from external DOS attacks.

## Proxy mode inspection

When a firewall policy's inspection mode is set to *proxy*, traffic flowing through the policy will be buffered by the FortiGate for inspection. This means that the packets for a file, email message, or web page will be held by the FortiGate until the entire payload is inspected for violations (virus, spam, or malicious web links). After FortiOS has finished the inspection, the payload is either released to the destination (if traffic is clean) or dropped and replaced with a replacement message (if traffic contains violations).

To optimize inspection, the policy can be configured to block or ignore files or messages that exceed a certain size. To prevent the receiving end user from timing out, client comforting can be applied, which allows small portions of the payload to be sent while it is undergoing inspection.

Proxy mode provides the most thorough inspection of the traffic; however, its thoroughness sacrifices performance, making its throughput slower than that of a flow-mode policy. Under normal traffic circumstances, the throughput difference between a proxy-based and flow-based policy is not significant.

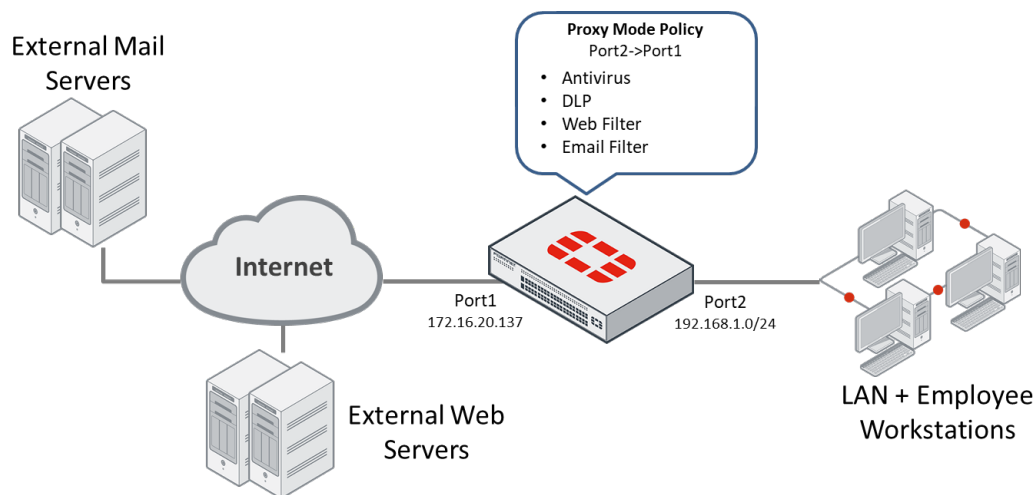
## Use case

Because proxy mode provides the most thorough inspection, it is recommended that you apply proxy inspection to policies where preventing a data leak or malicious content is critical.

The following scenarios demonstrate common use cases for proxy inspection.

### Scenario 1

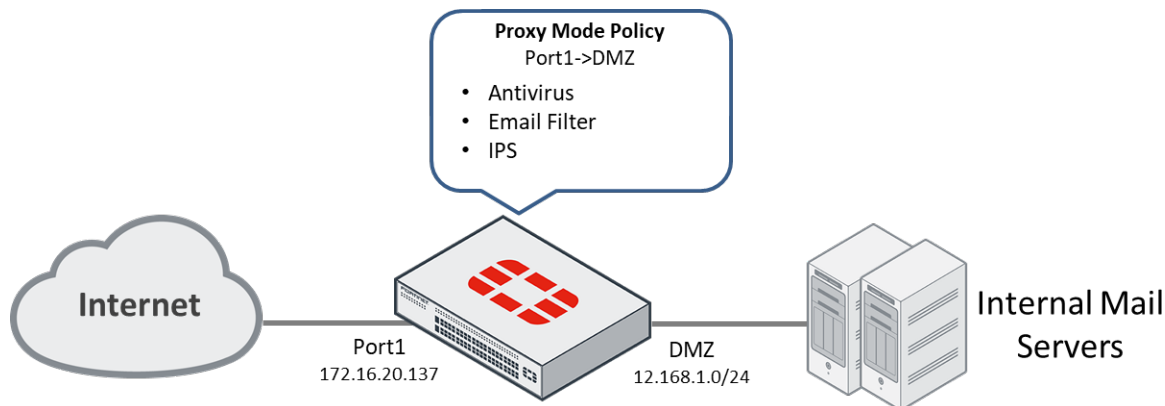
Your organization deals with sensitive data on a regular basis and a data leak would significantly harm your business. At the same time, you wish to protect your employees from malicious content, such as viruses and phishing emails, which could be used to gain access to your network and the sensitive data on your systems.



In this scenario, a proxy inspection policy is recommended to prioritize network security. We want traffic inspection to be as thorough as possible to avoid any data leaks from exiting the LAN and any malicious content from entering it. On this policy, we will apply the virus filter, DLP filter, Web Filter, and email filter all operating in proxy mode.

## Scenario 2

You have a corporate mail server in your domain, which is used by your employees for everyday business activities. You want to protect your employees from phishing emails and viruses. At the same time, you want to also protect your web servers from external attacks.



In this scenario, a proxy inspection policy is recommended to prioritize the safety of employee emails. Applying the antivirus and email filter in this mode allows us to most reliably filter out any malware and spam emails received by the mail servers via SMTP or MAPI. The IPS sensor can be used to prevent DOS attacks on the mail servers.

## Inspection mode feature comparison

The following table shows which UTM profile can be configured on a flow mode or proxy mode inspection policy. Some UTM profiles are hidden in the GUI, but can be configured using the CLI.

UTM Profile	Flow Mode Inspection Policy		Proxy Mode Inspection Policy	
	GUI	CLI	GUI	CLI
Antivirus	Yes (2)	Yes (2)	Yes	Yes
Application Control	Yes	Yes	Yes	Yes
CIFS Inspection	No	No	No (1)	Yes
Data Leak Prevention	No	Yes (3)	No	Yes
DNS Filter	Yes	Yes	Yes	Yes
Email Filter	No	Yes (4)	Yes	Yes
ICAP	No	No	Yes	Yes
Intrusion Prevention System	Yes	Yes	Yes	Yes
SSL/SSH Inspection	Yes	Yes	Yes	Yes
VoIP	Yes	Yes	Yes	Yes
Web Filter	Yes (5)	Yes (5)	Yes	Yes
Web Application Firewall	No	No	Yes	Yes

1. CIFS inspection cannot be configured via GUI.
2. Some Antivirus features are not supported in flow mode inspection. See [Inspection mode differences for antivirus on page 1088](#).
3. Some Data Leak Prevention features are not supported in Flow mode inspection. See [Inspection mode differences for data leak prevention on page 1089](#).
4. Some Email filter features are not supported in Flow mode inspection. See [Inspection mode differences for email filter on page 1090](#).
5. Some Web Filter features are not supported in Flow mode inspection. See [Inspection mode differences for web filter on page 1091](#).

## Inspection mode differences for antivirus

This section identifies the behavioral differences between antivirus operating in flow and proxy inspection.

### Feature comparison between antivirus inspection modes

The following table indicates which antivirus features are supported by their designated scan modes.

Part1	Replacement Message	Content Disarm	Mobile Malware	Virus Out-break	Sandbox Inspection	NAC Quar-antine
Proxy	Yes	Yes	Yes	Yes	Yes	Yes
Flow default mode	Yes*	No	No	No	Yes	Yes
Flow legacy mode	Yes*	No	Yes	Yes	Yes	Yes

\*IPS engine caches the URL and a replacement message will be presented after the second attempt.

Part 2	Archive Blocking	Emulator	Client Com-forting	Infection Quarantine	Heuristics	Treat EXE as Virus
Proxy	Yes	Yes	Yes	Yes (1)	Yes	Yes (2)
Flow default mode	No	No	No	No	No	No
Flow legacy mode	Yes	Yes	No	Yes (1)	Yes	Yes (2)

1. Only available on FortiGate models with HDD, or when FortiAnalyzer or FortiGate Cloud is connected and enabled.
2. Only applies to inspection on IMAP, POP3, SMTP, and MAPI protocols.

### Protocol comparison between antivirus inspection modes

The following table indicates which protocols can be inspected by the designated antivirus scan modes.

	HTTP	FTP	IMAP	POP3	SMTP	NNTP	MAPI	CIFS
Proxy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes*
Flow	Yes	Yes	Yes	Yes	Yes	No	No	Yes

\* Proxy mode antivirus inspection on CIFS protocol has the following limitations:

- Cannot detect infections within archive files
- Cannot detect oversized files
- Will block special archive types by default
- IPv6 is not supported

## Other antivirus differences between inspection modes

Flow default mode uses a hybrid scanning approach: it may use a pre-filtering database for malware detection in some circumstances as opposed to the full AV signature database in others. The scan method is determined by the AV engine algorithm that is based on the type of file being scanned. When a full AV scan is needed, the file is forwarded from the IPS engine to the scanunit daemon for processing.

Flow and proxy legacy modes use the full AV signature database, and the scanunit daemon scans the traffic.

Proxy mode uses pre-scanning and stream-based scanning for HTTP traffic. In default mode, the WAD daemon uses a stream-based approach, while legacy mode disables this stream-based approach.

Stream-based scanning provides the following AV improvements:

- Archive files (ZIP, GZIP, BZIP2, TAR, ISO) that exceed the oversize limit are uncompressed and scanned for infections.
- The contents of large archive files are scanned without having to buffer the entire file.
- Small files are scanned locally by the WAD daemon if only AV scanning is needed in the policy.
- File filtering on HTTP/HTTPS is handled locally by the WAD daemon.

This means that the overall memory usage is optimized when an archive file is scanned, and better security is achieved by scanning archives that would otherwise be bypassed.

However, stream-based scanning has limitations on the more complex features that it can scan. For the following features, traffic will be automatically handed off to the scanunit daemon for scanning (as in the case of legacy mode):

- Heuristic AV scan
- DLP
- Quarantine
- FortiGuard outbreak prevention and external block list
- Content disarm

### To configure the scan mode:

```
config antivirus profile
 edit <name>
 ...
 set scan-mode {default | legacy}
 next
end
```

## Inspection mode differences for data leak prevention

This section identifies the behavioral differences between data leak prevention (DLP) operating in flow and proxy inspection.

## Feature comparison between DLP inspection modes

The following table indicates which DLP filters are supported by their designated inspection modes.

	Credit Card Filter	SSN Filter	Regex Filter	File-Type Filter	File-Pattern Filter	Fingerprint Filter	Watermark Filter	Encrypted Filter	File-Size Filter
Proxy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Flow	Yes	Yes	Yes	No	Yes	No	No	Yes	Yes*

\*File-size filtering will only work if file size is present in the protocol exchange.

## Protocol comparison between DLP inspection modes

The following table indicates which protocols can be inspected by DLP based on the specified inspection modes.

	HTTP	FTP	IMAP	POP3	SMTP	NNTP	MAPI	CIFS
Proxy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Flow	Yes	Yes	Yes	Yes	Yes	No	No	No

## Inspection mode differences for email filter

This section identifies the behavioral differences between Email Filter operating in flow and proxy inspection.

## Feature comparison between Email Filter inspection modes

The following table indicates which Email Filters are supported by their designated inspection modes.

	SMTP	POP3	IMAP	MAPI
Proxy	Yes	Yes	Yes	Yes
Flow	Yes	Yes	Yes	No

## Feature comparison between Email Filter inspection modes

The following tables indicate which Email Filters are supported by the specified inspection modes for local filtering and FortiGuard-assisted filtering.

Local Filtering	Banned Word Check	Block/Allowlist	HELO/ EHLO DNS Check	Return Address DNS Check	DNSBL/ ORBL Check	MIME Header Check	File Filter
Proxy	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Flow	Yes	No	No	No	No	Yes	No



FortiGuard-Assisted Filtering	Phishing URL Check	Anti-Spam Blocklist Check	Submit Spam to FortiGuard	Spam Email Checksum Check	Spam URL Check
Proxy	Yes	Yes	Yes	Yes	Yes
Flow	No	No	No	No	No

## Inspection mode differences for web filter

This section identifies the behavioral differences between Web Filter operating in flow and proxy inspection.

### Feature comparison between Web Filter inspection modes

The following table indicates which Web Filter features are supported by their designated inspection modes.

	FortiGuard Category-Based Filter	Category Usage Quota	Override Blocked Categories	File Filter	Search Engines	Static URL Filter	Rating Option	Proxy Option
Proxy	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Flow	Yes (1)	No	Yes (2)	No	No	Yes	Yes	No

1. Local Category and Remote Category filters do not support the warning and authenticate actions.
2. Local Category and Remote Category filters cannot be overridden.

## SSL Inspection

Secure sockets layer (SSL) content scanning and inspection allows you to apply antivirus scanning, web filtering, and email filtering to encrypted traffic. You can apply SSL inspection profiles to firewall policies.

FortiOS includes four preloaded SSL/SSH inspection profiles, three of which are read-only and can be cloned:

- *certificate-inspection*
- *deep-inspection*
- *no-inspection*

The *custom-deep-inspection* profile can be edited, or you can create your own SSL/SSH inspection profiles.

Deep inspection (also known as SSL/SSH inspection) is typically applied to outbound policies where destinations are unknown. Depending on your policy requirements, you can configure the following:

- Which CA certificate will be used to decrypt the SSL encrypted traffic
- Which SSL protocols will be inspected
- Which ports will be associated with which SSL protocols for inspection
- Whether or not to allow invalid SSL certificates
- Whether or not SSH traffic will be inspected
- Which addresses or web category allowlists can bypass SSL inspection

The following topics provide information about SSL inspection:

- [Certificate inspection on page 1092](#)
- [Deep inspection on page 1093](#)
- [Protecting an SSL server on page 1096](#)
- [Ignoring the AUTH TLS command on page 1097](#)

## Certificate inspection

FortiGate supports certificate inspection. The default configuration has a built-in *certificate-inspection* profile which you can use directly. When you use certificate inspection, the FortiGate only inspects the headers up to the SSL/TLS layer.

If you do not want to deep scan for privacy reasons but you want to control web site access, you can use *certificate-inspection*.

## SSL inspection options

The following options are available when configuring an SSL inspection profile:

<b>Enable SSL inspection of</b>	Select <i>Multiple Clients Connecting to Multiple Servers</i> . This is normally used when inspecting outbound internet traffic
<b>Inspection method</b>	Select <i>SSL Certificate Inspection</i> .
<b>CA certificate</b>	Use the default <i>Fortinet_CA_SSL</i> certificate.
<b>Blocked certificates</b>	The FortiGate receives Botnet C&C SSL connections from FortiGuard that contain SHA1 fingerprints of malicious certificates. By default, these certificates are blocked. Click <i>View Blocked Certificates</i> to see a detailed list.
<b>Untrusted SSL certificates</b>	Configure the action to take when a server certificate is not issued by a trusted CA. <ul style="list-style-type: none"> <li>• <i>Allow</i>: Allow the untrusted server certificate. This is the default value.</li> <li>• <i>Block</i>: Block the session</li> <li>• <i>Ignore</i>: This option is for Full SSL inspection only. It re-signs the server certificate as trusted. When configured in the GUI for certificate inspection it has no effect and the setting is not saved.</li> </ul> Click <i>View Trusted CAs List</i> to see a list of the factory bundled and user imported CAs that are trusted by the FortiGate.
<b>Server certificate SNI check</b>	Check the SNI in the hello message with the CN or SAN field in the returned server certificate. <ul style="list-style-type: none"> <li>• <i>Enable</i>: If mismatched, use the CN in the server certificate to do URL filtering.</li> <li>• <i>Strict</i>: If mismatched, close the connection.</li> <li>• <i>Disable</i>: Server certificate SNI check is disabled.</li> </ul>

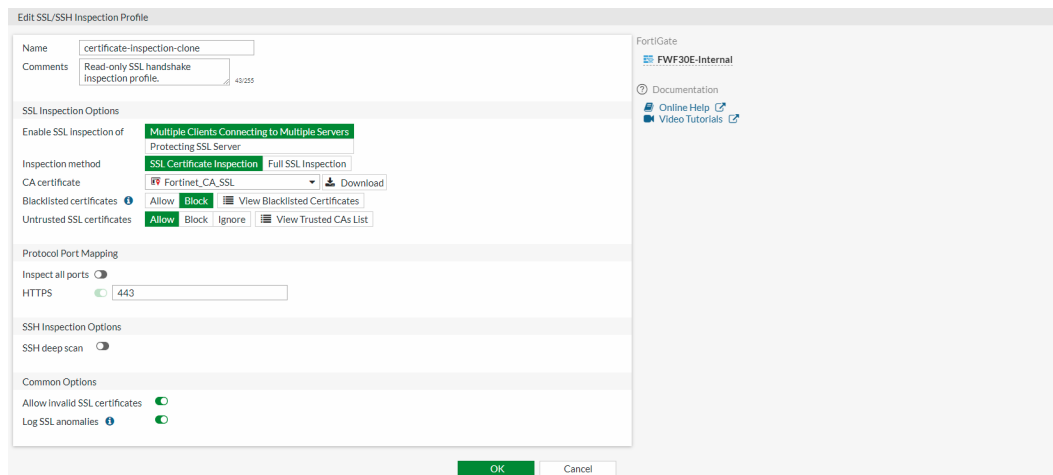
## Inspect non-standard HTTPS ports

The built-in *certificate-inspection* profile is read-only and only listens on port 443. If you want to make changes, you must create a new certificate inspection profile.

If you know the non-standard port that the web server uses, such as port 8443, you can add this port to the *HTTPS* field.

### To add a port to the inspection profile in the GUI:

1. Go to *Security Profiles > SSL/SSH Inspection*.
2. Create a new profile, or clone the default profile.
3. If you do not know what port is used in the HTTPS web server, under *Protocol Port Mapping* enable *Inspect All Ports*. If you know the port, such as port 8443, then set *HTTPS* to *443,8443*.



4. Configure the remaining settings as needed.
5. Click **OK**.

## Common options

Enable *Allow Invalid SSL Certificates* to allow invalid certificates, such as expired or revoked certificates.

By default, SSL anomalies logging is enabled. Logs are generated in the UTM log type under the SSL subtype when invalid certificates are detected.

## Deep inspection

You can configure address and web category allowlists to bypass SSL deep inspection.

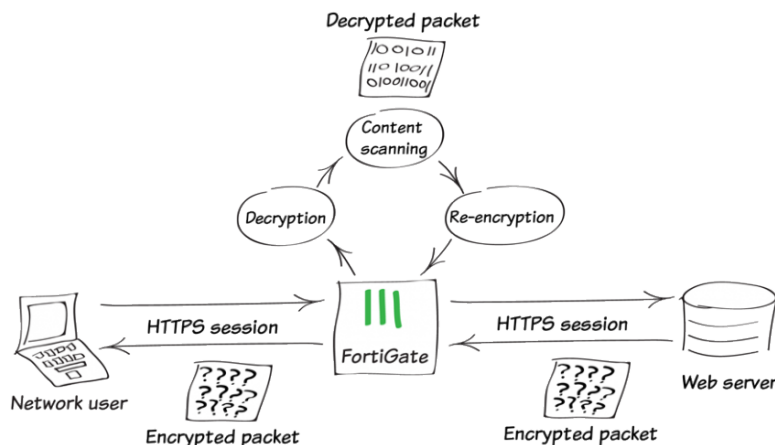
### Reasons for using deep inspection

While Hypertext Transfer Protocol Secure (HTTPS) offers protection on the Internet by applying Secure Sockets Layer (SSL) encryption to web traffic, encrypted traffic can be used to get around your network's normal defenses.

For example, you might download a file containing a virus during an e-commerce session, or you might receive a phishing email containing a seemingly harmless download that, when launched, creates an encrypted session to a command and control (C&C) server and downloads malware onto your computer. Because the sessions in these attacks are encrypted, they might get past your network's security measures.

When you use deep inspection, the FortiGate impersonates the recipient of the originating SSL session, then decrypts and inspects the content to find threats and block them. It then re-encrypts the content and sends it to the real recipient.

Deep inspection not only protects you from attacks that use HTTPS, it also protects you from other commonly-used SSL-encrypted protocols such as SMTPS, POP3S, IMAPS, and FTPS.



### Browser messages when using deep inspection

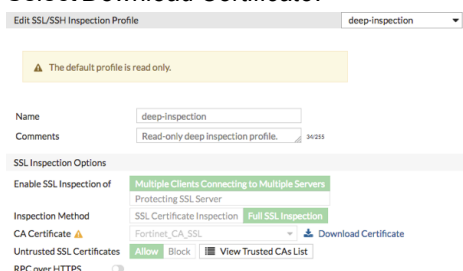
When FortiGate re-encrypts the content, it uses a certificate stored on the FortiGate such as *Fortinet\_CA\_SSL*, *Fortinet\_CA\_Untrusted*, or your own CA certificate that you uploaded.

Because there is no *Fortinet\_CA\_SSL* in the browser trusted CA list, the browser displays an untrusted certificate warning when it receives a FortiGate re-signed server certificate. To stop the warning messages, trust the FortiGate-trusted CA *Fortinet\_CA\_SSL* and import it into your browser.

After importing *Fortinet\_CA\_SSL* into your browser, if you still get messages about untrusted certificate, it must be due to *Fortinet\_CA\_Untrusted*. **Never** import the *Fortinet\_CA\_Untrusted* certificate into your browser.

### To import *Fortinet\_CA\_SSL* into your browser:

1. On the FortiGate, go to *Security Profiles > SSL/SSH Inspection* and select *deep-inspection*.
2. The default CA Certificate is *Fortinet\_CA\_SSL*.
3. Select *Download Certificate*.



4. On the client PC, double-click the certificate file and select *Open*.
5. Select *Install Certificate* to launch the *Certificate Import Wizard* and use the wizard to install the certificate into the *Trusted Root Certificate Authorities* store.  
If a security warning appears, select *Yes* to install the certificate.

### Exempt web sites from deep inspection

If you do not want to apply deep inspection for privacy or other reasons, you can exempt the session by address, category, or allowlist.

If you know the address of the server you want to exempt, you can exempt that address. You can exempt specific address type including IP address, IP address range, IP subnet, FQDN, wildcard-FQDN, and geography.

**Edit SSL/SSH Inspection Profile**

Name: custom-deep-inspection  
Comments: Customizable deep inspection profile. 27/255

**SSL Inspection Options**

Enable SSL Inspection of: Multiple Clients Connecting to Multiple Servers  
Inspection Method: SSL Certificate Inspection **Full SSL Inspection**  
CA Certificate: Fortinet\_CA\_SSL [Download Certificate](#)  
Untrusted SSL Certificates: **Allow** Block [View Trusted CAs List](#)  
RPC over HTTPS: ☐

**Protocol Port Mapping**

Inspect All Ports: ☒  
 HTTPS: ☒ 443  
 SMTPS: ☒ 465  
 POP3S: ☒ 995  
 IMAPS: ☒ 993  
 FTPS: ☒ 990

**Exempt from SSL Inspection**

Reputable Websites: ☐  
 Web Categories: +  
 Addresses: 172.16.200.99, gmail.com  
 Log SSL exemptions: ☒

**SSH Inspection Options**

SSH Deep Scan: ☐

[Apply](#)

If you want to exempt all bank web sites, an easy way is to exempt the *Finance and Banking* category which includes all finance and bank web sites identified in FortiGuard.

**Edit SSL/SSH Inspection Profile**

Name: custom-deep-inspection  
Comments: Customizable deep inspection profile. 27/255

**SSL Inspection Options**

Enable SSL Inspection of: Multiple Clients Connecting to Multiple Servers  
Inspection Method: SSL Certificate Inspection **Full SSL Inspection**  
CA Certificate: Fortinet\_CA\_SSL [Download Certificate](#)  
Untrusted SSL Certificates: **Allow** Block [View Trusted CAs List](#)  
RPC over HTTPS: ☐

**Protocol Port Mapping**

Inspect All Ports: ☒  
 HTTPS: ☒ 443  
 SMTPS: ☒ 465  
 POP3S: ☒ 995  
 IMAPS: ☒ 993  
 FTPS: ☒ 990

**Exempt from SSL Inspection**

Reputable Websites: ☐  
 Web Categories: Finance and Banking  
 Addresses: +  
 Log SSL exemptions: ☒

**SSH Inspection Options**

SSH Deep Scan: ☐

[Apply](#)

If you want to exempt commonly trusted web sites, you can bypass the SSL allowlist in the SSL/SSH profile. The allowlist includes common web sites trusted by FortiGuard. Simply enable *Reputable Websites*.

## Protecting an SSL server

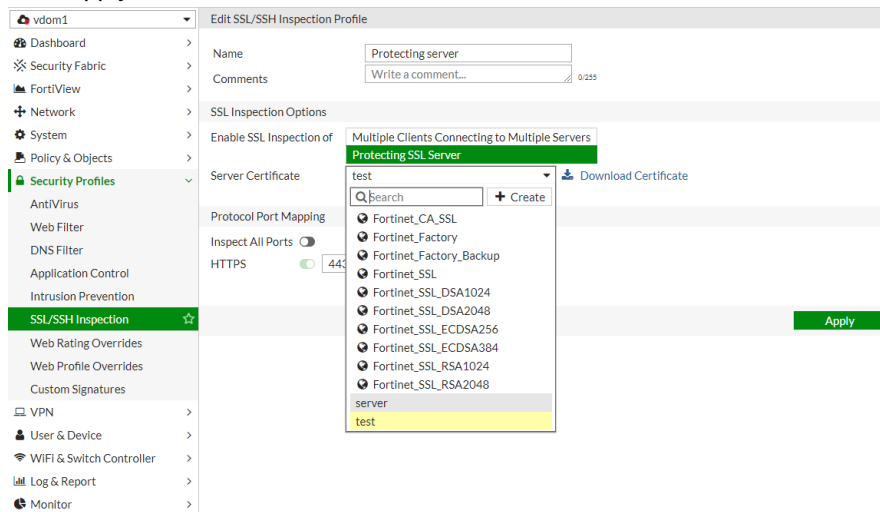
You typically use the FortiGate *Protecting SSL Server* profile as an inbound policy for clients on the internet that access the server through the internal side of the FortiGate.

*Protecting SSL Server* uses a server certificate to protect a single server.

You can use *Protecting SSL Server* if you do not want a client on the internet to directly access your internal server, and you want the FortiGate to simulate your real server.

**To upload a server certificate into FortiGate and use that certificate in the SSL/SSH inspection profile:**

1. Go to *System > Certificates*.
2. Select *Import > Local Certificate* and upload the certificate.
3. Go to *Security Profiles > SSL/SSH Inspection* and edit or create a new profile.
4. For *Enable SSL Inspection of*, select *Protecting SSL Server*.
5. For *Server Certificate*, select the local certificate you imported.

6. Click *Apply*.

When you apply the *Protecting SSL Server* profile in a policy, the FortiGate will send the server certificate to the client as your server does.

## Ignoring the AUTH TLS command

If the FortiGate receives an AUTH TLS (PBSZ and PROT) command before receiving plain text traffic from a decrypted device, by default, it will expect encrypted traffic, determine that the traffic belongs to an abnormal protocol, and bypass the traffic.

When the `ssl-offloaded` command is enabled, the AUTH TLS command is ignored, and the traffic is treated as plain text rather than encrypted data. SSL decryption and encryption are performed by an external device.

### To enable SSL offloading:

```
config firewall profile-protocol-options
 edit "test"
 config ftp
 set ssl-offloaded yes
 end
 config imap
 set ssl-offloaded yes
 end
 config pop3
 set ssl-offloaded yes
 end
 config smtp
 set ssl-offloaded yes
 end
 next
end
```

## SSH traffic file scanning

FortiGate can buffer, scan, log, or block files sent over SSH traffic (SCP and SFTP) depending on the file size, type, or contents (such as viruses or sensitive content).



This feature is supported in proxy-based inspection mode. It is currently not supported in flow-based inspection mode.

---

You can configure the following SSH traffic settings in the CLI:

- Protocol options
- Filter profile (SCP block/log options and file filter)
- DLP sensor
- Antivirus (profile and quarantine options)

### To configure SSH protocol options:

```
config firewall profile-protocol-options
 edit "protocol"
 config ssh
 set options [oversize | clientcomfort | servercomfort]
 set comfort-interval [1 - 900]
 set comfort-amount [1 - 65535]
 set oversize-limit [1 - 798]
 set uncompressed-oversize-limit [0 - 798]
 set uncompressed-nest-limit [2 - 100]
 set scan-bzip2 [enable | disable]
 end
 next
end
```

### To configure SCP block and log options:

```
config ssh-filter profile
 edit "ssh-test"
 set block scp
 set log scp
 next
end
```

### To configure the SSH file filter:

```
config ssh-filter profile
 edit "ssh-test"
 config file-filter
 set status [enable | disable]
 set log [enable | disable]
 set scan-archive-contents [enable | disable]
 config entries
 edit "1"
 set comment ''
 set action [block | log]
 next
 end
 next
end
```



```
 set direction [incoming | outgoing | any]
 set password-protected [yes | any]
 set file-type "msoffice"
 next
end
end
next
end
```

**To configure the DLP sensor:**

```
config dlp sensor
 edit "test"
 set full-archive-proto ssh
 set summary-proto ssh
 config filter
 edit 1
 set proto ssh
 next
 end
 next
end
```

**To configure the antivirus profile options:**

```
config antivirus profile
 edit "av"
 config ssh
 set options [scan | avmonitor | quarantine]
 set archive-block [encrypted | corrupted | partiallycorrupted | multipart |
nested | mailbomb | fileslimit | timeout | unhandled]
 set archive-log [encrypted | corrupted | partiallycorrupted | multipart | nested
| mailbomb | fileslimit | timeout | unhandled]
 set emulator [enable | disable]
 set outbreak-prevention [disabled | files | full-archive]
 end
 next
end
```

**To configure the antivirus quarantine options:**

```
config antivirus quarantine
 set drop-infected ssh
 set store-infected ssh
 set drop-blocked ssh
 set store-blocked ssh
 set drop-heuristic ssh
 set store-heuristic ssh
end
```

## Sample logs

### SCP traffic blocked by ssh-filter profile:

```
1: date=2019-07-24 time=10:34:42 logid="1601061010" type="utm" subtype="ssh" eventtype="ssh-channel" level="warning" vd="vdom1" eventtime=1563989682560488314 tz="-0700" policyid=1 sessionid=2693 profile="ssh-test" srcip=10.1.100.11 srcport=33044 dstip=172.16.200.44 dstport=22 srcintf="port1" srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" proto=6 action="blocked" direction="outgoing" login="root" channeltype="scp"
```

### SCP traffic blocked by file-filter:

```
1: date=2019-07-24 time=10:36:44 logid="1900064000" type="utm" subtype="file-filter" eventtype="file-filter" level="warning" vd="vdom1" eventtime=1563989804387444023 tz="-0700" policyid=1 sessionid=2732 srcip=10.1.100.11 srcport=33048 srcintf="port1" srcintfrole="undefined" dstip=172.16.200.44 dstport=22 dstintf="port3" dstintfrole="undefined" proto=6 service="SSH" subservice="SCP" profile="ssh-test" direction="incoming" action="blocked" filtername="1" filename="test.xls" filesize=13824 filetype="msoffice" msg="File was blocked by file filter."
```

### SFTP traffic blocked by file-filter:

```
1: date=2019-07-24 time=10:43:58 logid="1900064000" type="utm" subtype="file-filter" eventtype="file-filter" level="warning" vd="vdom1" eventtime=1563990238339440605 tz="-0700" policyid=1 sessionid=2849 srcip=10.1.100.11 srcport=33056 srcintf="port1" srcintfrole="undefined" dstip=172.16.200.44 dstport=22 dstintf="port3" dstintfrole="undefined" proto=6 service="SSH" subservice="SFTP" profile="ssh-test" direction="incoming" action="blocked" filtername="1" filename="test.xls" filesize=13824 filetype="msoffice" msg="File was blocked by file filter."
```

### SCP traffic blocked by dlp sensor:

```
1: date=2019-07-24 time=10:42:42 logid="0954024576" type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="vdom1" eventtime=1563990162266253784 tz="-0700" filteridx=1 filtername="test" dlpextra="builtin-patterns" filtertype="file-type" filtercat="file" severity="medium" policyid=1 sessionid=2838 epoch=1425775843 eventid=0 srcip=10.1.100.11 srcport=33054 srcintf="port1" srcintfrole="undefined" dstip=172.16.200.44 dstport=22 dstintf="port3" dstintfrole="undefined" proto=6 service="SSH" subservice="SFTP" filetype="msoffice" direction="incoming" action="block" filename="test.xls" filesize=13824 profile="test"
```

### SFTP traffic blocked by dlp sensor:

```
1: date=2019-07-24 time=10:41:23 logid="0954024576" type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="vdom1" eventtime=1563990083875731367 tz="-0700" filteridx=1 filtername="test" dlpextra="builtin-patterns" filtertype="file-type" filtercat="file" severity="medium" policyid=1 sessionid=2809 epoch=1425775842 eventid=0 srcip=10.1.100.11 srcport=33052 srcintf="port1" srcintfrole="undefined" dstip=172.16.200.44 dstport=22 dstintf="port3" dstintfrole="undefined" proto=6 service="SSH" subservice="SCP" filetype="msoffice" direction="incoming" action="block" filename="test.xls" filesize=13824 profile="test"
```

**SCP traffic blocked by antivirus profile:**

```
1: date=2019-07-24 time=10:45:57 logid="0211008192" type="utm" subtype="virus"
eventtype="infected" level="warning" vd="vdom1" eventtime=1563990357330463670 tz="-0700"
msg="File is infected." action="blocked" service="SSH" subservice="SCP" sessionid=2875
srcip=10.1.100.11 dstip=172.16.200.44 srcport=33064 dstport=22 srcintf="port1"
srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" policyid=1 proto=6
direction="incoming" filename="eicar.exe" checksum="53badd68" quarskip="No-skip"
virus="EICAR_TEST_FILE" dtype="Virus" ref="http://www.fortinet.com/ve?vn=EICAR_TEST_FILE"
virusid=2172 profile="av"
analyticscksum="7fc2dfc5a2247d743556ef59abe3e03569a6241e2b1e44b9614fc764847fb637"
analyticssubmit="false" crscore=50 craction=2 crlevel="critical"
```

**SFTP traffic blocked by antivirus profile:**

```
2: date=2019-07-24 time=10:45:46 logid="0211008192" type="utm" subtype="virus"
eventtype="infected" level="warning" vd="vdom1" eventtime=1563990346334781409 tz="-0700"
msg="File is infected." action="blocked" service="SSH" subservice="SFTP" sessionid=2874
srcip=10.1.100.11 dstip=172.16.200.44 srcport=33062 dstport=22 srcintf="port1"
srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" policyid=1 proto=6
direction="incoming" filename="eicar.exe" checksum="53badd68" quarskip="No-skip"
virus="EICAR_TEST_FILE" dtype="Virus" ref="http://www.fortinet.com/ve?vn=EICAR_TEST_FILE"
virusid=2172 profile="av"
analyticscksum="7fc2dfc5a2247d743556ef59abe3e03569a6241e2b1e44b9614fc764847fb637"
analyticssubmit="false" crscore=50 craction=2 crlevel="critical"
```

**Antivirus quarantine list triggered by infected files sent over SCP/SFTP:**

CHECKSUM	SIZE	FIRST-TIMESTAMP	LAST-TIMESTAMP	SERVICE	STATUS	DC	TTL
53badd68	12939	2019-07-24 10:45	2019-07-24 10:45	SSH	Infected	1	FOREVER
'eicar.exe'							'EICAR_TEST_FILE'

## Overrides

Web filter configuration can be separated into profile configuration and profile overrides.

You can also override web filter behavior based on the FortiGuard website categorization:

- Use alternate categories (web rating overrides): this method manually assigns a specific website to a different Fortinet category or a locally-created category.
- Use alternate profiles: configured users or IP addresses can use an alternative web filter profile when attempting to access blocked websites.



Some features of this functionality require a subscription to FortiGuard Web Filtering.

The following topics provide information about web overrides:

- [Web rating override on page 1102](#)
- [Web profile override on page 1107](#)

## Web rating override

Web rating overrides allow you to add specific URLs to both FortiGuard and custom web ratings categories. The action for each category can be configured in a web filter profile. See [FortiGuard filter on page 954](#) for more information.

If a URL is in multiple enabled categories, the order of precedence is local categories, then remote categories, and then FortiGuard categories.



The custom category *Allow* action will have different effects depending on the inspection mode in the policy that the web profile is used in:

- In flow-based inspection mode: The category is disabled and has no impact on the web filter. The action of the next category in the order of preference is applied.
- In proxy-based inspection mode: The category is allowed.

In SSL/SSH inspection profiles, custom categories must be explicitly selected to be exempt from SSL inspection. In proxy addresses, custom categories must be explicitly selected as URL categories for them to apply. In both settings, if a URL is in multiple selected categories, the order of precedence is local categories, then remote categories, and then FortiGuard categories.



Web rating override requires a FortiGuard license.

## Web filter profiles

In this example, [www.fortinet.com](http://www.fortinet.com) is added to both a custom, or local, category (*Seriously*) and an external threat feed, or remote, category (*OnAworkComputer*). The local category action is set to *Monitor*, while the remote category action is set to *Block*. When a user browses to [www.fortinet.com](http://www.fortinet.com), the local category action takes precedence over both the remote category and the FortiGuard category (*Information Technology*), so the *Monitor* action is taken.

### To create a custom category in the GUI:

1. Go to *Security Profiles > Web Rating Overrides*.
2. Click *Custom Categories*, then click *Create New*.
3. Enter a name for the category, and adjust the *Status* as needed.

4. Click *OK*.

### To create a web rating override in the GUI:

1. Go to *Security Profiles > Web Rating Overrides* and click *Create New*.
2. Enter the URL to override.
3. Optionally, click *Lookup rating* to see what its current rating is, if it has one.

4. Select the new *Category* and *Sub-Category* for the override.

The screenshot shows the 'New Web Rating Override' dialog. The URL field contains 'www.fortinet.com'. The Category dropdown is set to 'General Interest - Business' and the Sub-Category dropdown is set to 'Information Technology'. In the 'Override to' section, the Category dropdown is set to 'Custom Categories' and the Sub-Category dropdown is set to 'Seriously'. At the bottom, there are 'OK' and 'Cancel' buttons.

5. Click **OK**.

**To create a new FortiGuard category threat feed in the GUI:**

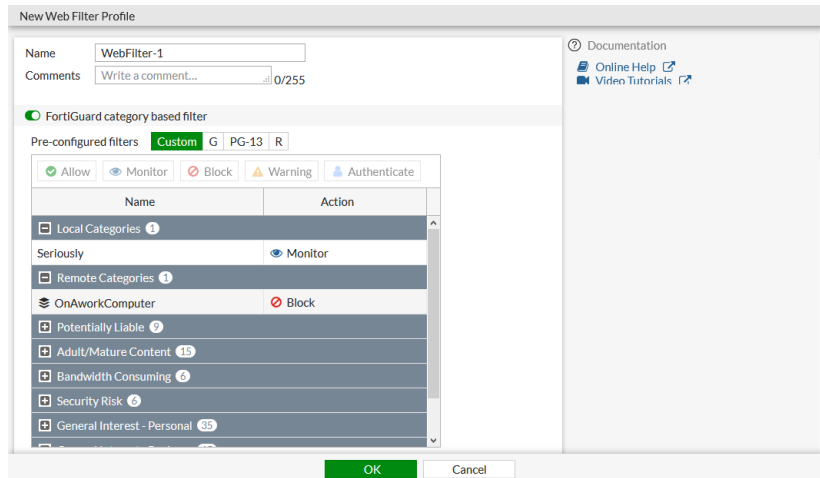
1. Go to *Security Fabric > External Connectors* and click *Create New*.
2. In the *Threat Feeds* section, click *FortiGuard Category*.
3. Enter a name for the threat feed, such as *OnAworkComputer*.
4. Enter the *URI of external resource*.

The screenshot shows the 'New External Connector' dialog. The 'Threat Feeds' section has a 'FortiGuard Category' icon. The 'Connector Settings' section includes: Name (OnAworkComputer), URI of external resource (https://192.168.0.5/lists/blocklist.txt), HTTP basic authentication (5), Refresh Rate (Minutes (1 - 43200)), and Comments (0/255). At the bottom, there are 'OK' and 'Cancel' buttons.

5. Configure the remaining settings as needed, then click **OK**.

**To use the new categories in a web filter profile in the GUI:**

1. Go to *Security Profiles > Web Filter* and create or edit a web filter profile. See [FortiGuard filter on page 954](#) for more information.
2. Enable *FortiGuard category based filter*
3. Set the action for the *Seriously* category in the *Local Categories* group to *Monitor*.
4. Set the action for the *OnAworkComputer* category in the *Remote Categories* group to *Block*.



5. Configure the remaining settings are required, then click **OK**.

### To use local and remote categories in a web filter profile in the CLI:

1. Create the custom category and add a URL to it:

```
config vdom
 edit root
 config webfilter ftgd-local-cat
 edit "Seriously"
 set id 140
 next
 end
 config webfilter ftgd-local-rating
 edit "www.fortinet.com"
 set rating 140
 next
 end
 next
end
```

2. Create a *FortiGuard Category Threat Feed* external connector to import an external blocklist.

```
config global
 config system external-resource
 edit "OnAworkComputer"
 set category 192
 set resource "https://192.168.0.5/lists/blocklist.txt"
 next
 end
end
```

3. Enable the new category in a web filter profile. See [FortiGuard filter on page 954](#) for details. Custom local categories have an ID range of 140 to 191. Remote categories have an ID range of 192 to 221.

```
config vdom
 edit root
 config webfilter profile
 edit "WebFilter-1"
 config ftgd-wf
 unset options
 end
 end
 end
 end
```

```

config filters
 edit 12
 set category 12
 set action warning
 next
 ...
 edit 23
 set action warning
 next
 edit 140
 set category 140
 next
 edit 192
 set category 192
 set action block
 next
end
end
next
end
next
end

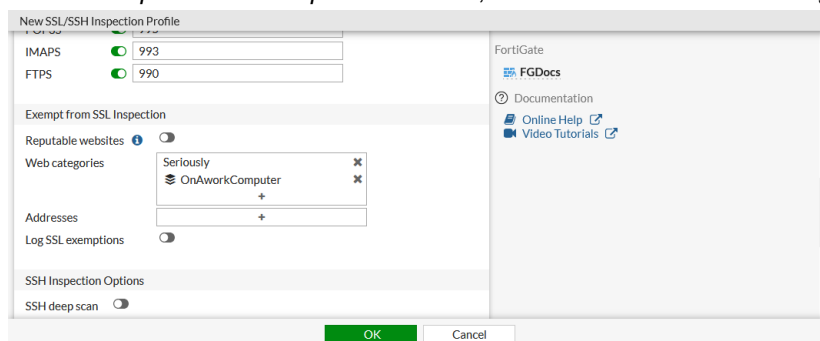
```

When a filter is added for the local and remote categories (140 and 192 in this example), the default action is monitor.

## SSL/SSH inspection profiles

To use local and remote categories in an SSL/SSH inspection profile to exempt them from SSL inspection in the GUI:

1. Go to *Security Profiles > SSL/SSH Inspection*.
2. Create a new profile or edit an existing one.
3. Ensure that *Inspection method* is *Full SSL Inspection*.
4. In the *Exempt from SSL Inspection* section, add the local and remote categories to the *Web categories* list .



5. Configure the remaining settings as required, then click **OK**.

To use local and remote categories in an SSL/SSH inspection profile to exempt them from SSL inspection in the CLI:

```

config vdom
 edit root

```

```

config firewall ssl-ssh-profile
 edit "SSL_Inspection"
 config https
 set ports 443
 set status deep-inspection
 end
 ...
 config ssl-exempt
 edit 1
 set fortiguard-category 140
 next
 edit 2
 set fortiguard-category 192
 next
 end
 next
end
next
end

```

## Proxy addresses

To use local and remote categories in a proxy address in the GUI:

1. Go to *Policy & Objects > Addresses* and click *Create New > Address*, or edit an existing proxy address.
2. Set *Category* to *Proxy Address*.
3. Set *Type* to *URL Category*.
4. In the *URL Category*, add the local and remote categories.

5. Configure the remaining settings as required, then click **OK**.

To use local and remote categories in a proxy address in the CLI:

```

config vdom
 edit root
 config firewall proxy-address
 edit "proxy_override"
 set type category
 set host "all"
 set category 140 192
 set color 23
 next
 end
 end

```

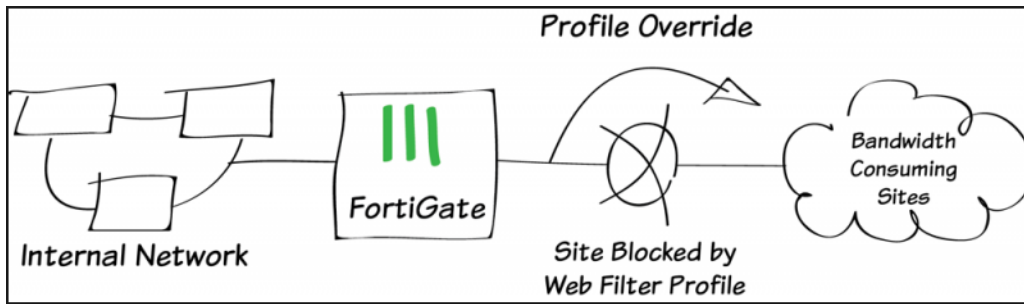


```
next
end
```

## Web profile override

You can use the following profile override methods:

- Administrative override
- Allow users to override blocked categories



### Administrative override

Administrators can grant temporary access to sites that are otherwise blocked by a web filter profile. You can grant temporary access to a user, user group, or source IP address. You can set the time limit for days, hours, or minutes. The default is 15 minutes.

When the administrative web profile override is enabled, a blocked access page or replacement message does not appear, and authentication is not required.

### Scope range

You can choose one of the following scope ranges:

- User: authentication for permission to override is based on whether or not the user is using a specific user account.
- User group: authentication for permission to override is based on whether or not the user account supplied as a credential is a member of the specified user group.
- Source IP: authentication for permission to override is based on the IP address of the computer that was used to authenticate. This would be used for computers that have multiple users. For example, if a user logs on to the computer, engages the override by using their credentials, and then logs off, anyone who logs on with an account on that computer would be using the alternate override web filter profile.



When you enter an IP address in the administrative override method, only individual IP addresses are allowed.

### Differences between IP and identity-based scope

Using the IP scope does not require using an identity-based policy.

When using the administrative override method and IP scope, you might not see a warning message when you change from using the original web filter profile to using the alternate profile. There is no requirement for credentials from the user so, if allowed, the page will just appear in the browser.

## Example of configuring a web profile administrative override

This example describes how to override a *webfilter* profile with a *webfilter\_new* profile.

### To configure web profile administrative override using the GUI:

1. Go to *Security Profiles > Web Profile Overrides*.
2. Click *Create New*.

+ Create New

Edit

Delete

Search

Q

Type

Initiator

Scope

Original Profile

New Profile

Status

Expires

No matching entries found

The *New Administrative Override* pane opens.

3. Configure the administrative override:
  - a. For *Scope Range*, click *Source IP*.
  - b. In the *Source IP* field, enter the IP address for the client computer (10.1.100.11 in this example).
  - c. In the *Original Profile* dropdown, select *webfilter*.
  - d. In the *New Profile* dropdown, select *webfilter\_new*.

In the *Minutes* field, the default 15 minutes appears, which is the desired duration for this example.

Edit Administrative Override

Scope Range

User

User Group

Source IP

Source IP

10.1.100.11

Original Profile

WEB

webfilter

New Profile

WEB

webfilter\_new

Expires

0

Days

0

Hours

15

Minutes

(Expires: 2019/07/03 16:17:00)

OK

Cancel

4. Click *OK*. The list of web profile overrides appears.  
The actual expiration time displays instead of the number of minutes.

<div><div>+ Create New</div><div><div>✎ Edit</div><div>🗑 Delete</div></div><div><div>Search</div><div>🔍</div></div></div>						
Type ▾	Initiator ▾	Scope ▾	Original Profile ▾	New Profile ▾	Status ▾	Expires ▾
Admin	admin	10.1.100.11	webfilter	webfilter_new	Enabled	2019/07/03 16:17:00

### To configure web profile administrative override using the CLI:

```
config webfilter override
edit 1
 set status enable
 set scope ip
 set old-profile "webfilter"
 set new-profile "webfilter_new"
 set expires 2019/04/10 14:33:00
 set initiator "admin"
 set ip 10.1.100.11
next
end
```

## Allow users to override blocked categories

For both override methods, the scope ranges (for specified users, user groups, or IP addresses) allow sites blocked by web filtering profiles to be overridden for a specified length of time.

But there is a difference between the override methods when the users or user group scope ranges are selected. In both cases, you would need to apply the user or user group as source in the firewall policy. With administrative override, if you do not apply the source in the firewall policy, the traffic will not match the override and will be blocked by the original profile. With *Allow users to override blocked categories*, the traffic will also be blocked, but instead of displaying a blocking page, the following message appears:



### Web Filter Block Override

If you have been granted override creation privileges by your administrator, you can enter your username and password here to gain immediate access to the blocked web-page. If you do not have these privileges, please contact your administrator to gain access to the web-page.  
Only user based overrides are allowed and you do not appear to be authenticated with the system. Please contact your administrator.

When you choose the user group scope, once one user overrides, it will affect the other users in the group when they attempt to override. For example, user1 and user2 both belong to the local\_user group. Once user1 successfully overrides, this will generate an override entry for the local\_user group instead of one specific user. This means that if user2 logs in from another PC, they can override transparently.

## Ask feature

This option is only available in the *Allow users to override blocked categories* method. It configures the message page to have the user choose which scope they want to use. Normally on the message page, the scope options are greyed out and not editable. In the following example, the *Scope* is predefined with *IP*.



### Web Filter Block Override

If you have been granted override creation privileges by your administrator, you can enter your username and password here to gain immediate access to the blocked web-page. If you do not have these privileges, please contact your administrator to gain access to the web-page.

Username:

Password:

Scope:

New Profile:

Duration:  (Days)  (Hours)  
 (Minutes)

When the ask option is enabled (through the *Switch applies to* field in the GUI), the *Scope* dropdown is editable. Users can choose one of the following:

- User
- User Group
- IP



### Web Filter Block Override

If you have been granted override creation privileges by your administrator, you can enter your username and password here to gain immediate access to the blocked web-page. If you do not have these privileges, please contact your administrator to gain access to the web-page.

Username:

Password:

Scope:

New Profile:

Duration:  (Days)  (Hours)  (Minutes)



*User* and *User Group* are only available when there is a user group in the firewall policy. You must specify a user group as a source in the firewall policy so the scope includes *User* and *User Group*; otherwise, only the IP option will be available.

### Other features

Besides the scope, there are some other features in *Allow users to override blocked categories*.

### Apply to group(s)

Individual users can not be selected. You can select one or more of the user groups recognized by the FortiGate. They can be local to the system or from a third party authentication device, such as an AD server through FSSO.

### Switch duration

Administrative override sets a specified time frame that is always used for that override. The available options in *Allow users to override blocked categories* are:

- *Predefined*: the value entered is the set duration (length of time in days, hours, or minutes) that the override will be in effect. If the duration variable is set to 15 minutes, the length of the override will always be 15 minutes. The option will be visible in the override message page, but the setting will be greyed out.
- *Ask*: the user has the option to set the override duration once it is engaged. The user can set the duration in terms of days, hours, or minutes.

### Example of creating a web profile users override

This example describes how to allow users in the *local\_group* to override the *webfilter\_new* profile.

#### To allow users to override blocked categories using the GUI:

1. Go to *Security Profiles > Web Filter*.
2. Click *Create New*.

3. Under the *Category Usage Quota* section, toggle on *Allow users to override blocked categories*.

Category Usage Quota ⓘ

+ Create New Edit Delete

Category ⌵	Total quota ⌵
No results	

☒ Allow users to override blocked categories

4. Configure the web filter profile:
- Click the *Groups that can override* field, and select a group (*local\_group* in this example).
  - Click the *Profile Name* field, and select the *webfilter\_new* profile.
  - For the *Switch applies to* field, click *IP*.
  - For the *Switch Duration* field, click *Predefined*. The default 15 minutes appears, which is the desired duration for this example.
  - Configure the rest of the profile as needed.

☒ Allow users to override blocked categories

Groups that can override

Profile Name

Switch applies to

Switch Duration

0 day(s) 0 hour(s) 15 minute(s)

5. Click *OK*.

## Custom signatures

You can create the following custom signatures and apply them to firewall policies:

- IPS signature
- Application signature
- Application group

The following topic provides information about custom signatures:

- [Application groups in policies on page 1111](#)

## Application groups in policies

This feature provides an application group command for firewall shaping policies.

The following CLI command is used:

```
config firewall shaping-policy
edit 1
set app-group <application group>...
.....
```

next  
end

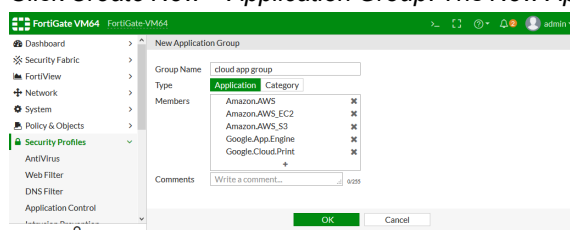
## Example

In this example, there are two traffic shaping policies:

- Policy 1 is for traffic related to cloud applications that has high priority.
- Policy 2 is for other traffic and has low priority.

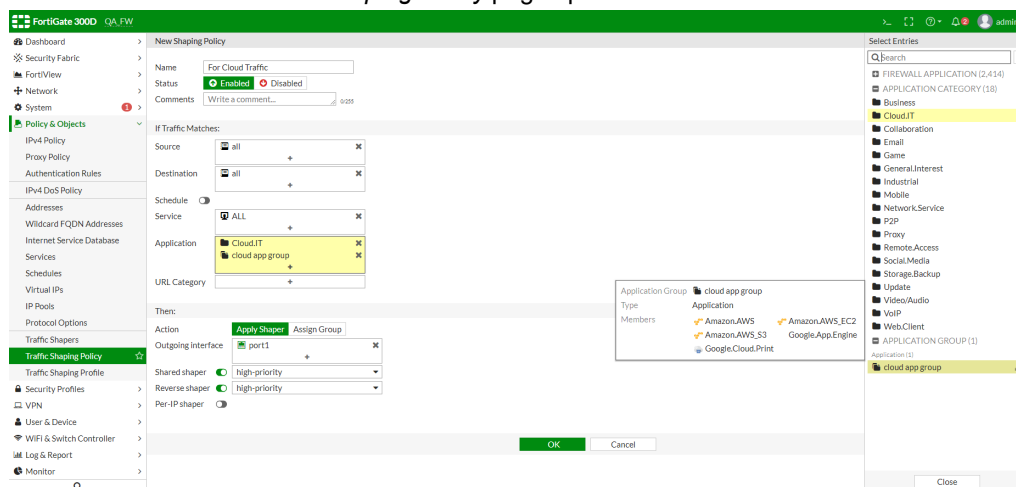
### To create the shaping policies using the GUI:

1. Configure an application group for cloud applications:
  - a. Go to *Security Profiles > Application Signatures*.
  - b. Click *Create New > Application Group*. The *New Application Group* page opens.



- c. Enter a name for the group, select the type, and then add the group the members.
- d. Click **OK**.

2. Create the shaping policy for the high priority cloud application traffic:
  - a. Go to *Policy & Objects > Traffic Shaping Policy*.
  - b. Click *Create New*. The *New Shaping Policy* page opens.

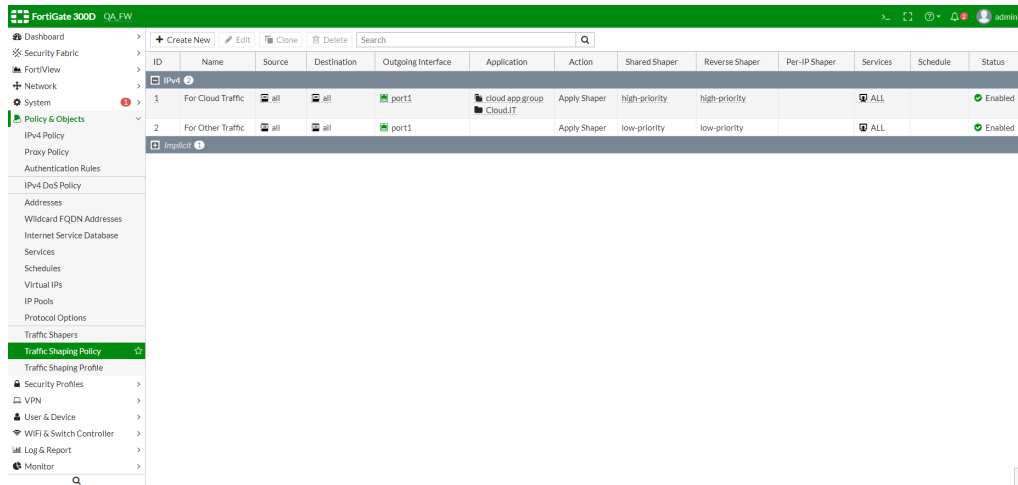


- c. Configure the shaping policy, selecting the previously created cloud application group, and setting both the *Shared shaper* and *Reverse shaper* to *high-priority*.
- d. Click **OK**.



At least one firewall policy must have application control enabled for the applications to match any policy traffic.

3. Create the shaping policy for all other traffic, setting both the *Shared shaper* and *Reverse shaper* to *low-priority*.



## To create the shaping policies using the CLI:

1. Configure an application group for cloud applications:

```
config application group
 edit "cloud app group"
 set application 27210 36740 35944 24467 33048
 next
end
```

2. Create the shaping policies for the high priority cloud application traffic and the other, low priority traffic:

```
config firewall shaping-policy
 edit 1
 set name "For Cloud Traffic"
 set service "ALL"
 set app-category 30
 set app-group "cloud app group"
 set dstintf "port1"
 set traffic-shaper "high-priority"
 set traffic-shaper-reverse "high-priority"
 set srcaddr "all"
 set dstaddr "all"
 next
 edit 2
 set name "For Other Traffic"
 set service "ALL"
 set dstintf "port1"
 set traffic-shaper "low-priority"
 set traffic-shaper-reverse "low-priority"
 set srcaddr "all"
 set dstaddr "all"
 next
end
```

# VPN

Virtual Private Network (VPN) technology lets remote users connect to private computer networks to gain access to their resources in a secure way. For example, an employee traveling or working at home can use a VPN to securely access the office network through the Internet.

Instead of remotely logging into a private network using an unencrypted and unsecured Internet connection, using a VPN ensures that unauthorized parties cannot access the office network and cannot intercept information going between the employee and the office. Another common use of a VPN is to connect the private networks of multiple offices.

Fortinet offers VPN capabilities in the FortiGate Unified Threat Management (UTM) appliance and in the FortiClient Endpoint Security suite of applications. You can install a FortiGate unit on a private network and install FortiClient software on the user's computer. You can also use a FortiGate unit to connect to the private network instead of using FortiClient software.

The following sections provide information about VPN:

- [IPsec VPNs on page 1114](#)
- [SSL VPN on page 1370](#)

## IPsec VPNs

The following sections provide instructions on configuring IPsec VPN connections in FortiOS 6.2.15.

- [General IPsec VPN configuration on page 1114](#)
- [Site-to-site VPN on page 1139](#)
- [Remote access on page 1199](#)
- [Aggregate and redundant VPN on page 1245](#)
- [Overlay Controller VPN \(OCVPN\) on page 1283](#)
- [ADVPN on page 1310](#)
- [Other VPN topics on page 1341](#)
- [VPN IPsec troubleshooting on page 1363](#)

## General IPsec VPN configuration

The following sections provide instructions on general IPsec VPN configurations:

- [Network topologies on page 1115](#)
- [Phase 1 configuration on page 1115](#)
- [Phase 2 configuration on page 1131](#)
- [VPN security policies on page 1135](#)
- [Blocking unwanted IKE negotiations and ESP packets with a local-in policy on page 1138](#)



## Network topologies

The topology of your network will determine how remote peers and clients connect to the VPN and how VPN traffic is routed.

Topology	Description
Site-to-Site	Standard one-to-one VPN between two FortiGates. See <a href="#">Site-to-site VPN on page 1139</a> .
Hub and spoke/ADVPN	One central FortiGate (hub) has multiple VPNs to other remote FortiGates (spokes). In ADVPN, shortcuts can be created between spokes for direct communication. See <a href="#">ADVPN on page 1310</a> .
OCVPN	Fortinet's cloud based solution for automating VPN setup between devices registered to the same account. See <a href="#">Overlay Controller VPN (OCVPN) on page 1283</a> .
FortiClient dialup	Typically remote FortiClient dialup clients use dynamic IP addresses through NAT devices. The FortiGate acts as a dialup server allowing dialup VPN connections from multiple sources. See <a href="#">FortiClient as dialup client on page 1205</a> .
FortiGate dialup	Similar to site-to-site except one end is a dialup server and the other end is a dialup client. This facilitates scenarios in which the remote dialup end has a dynamic address, or does not have a public IP, possibly because it is behind NAT. See <a href="#">FortiGate as dialup client on page 1199</a> .
Aggregate VPN	Natively support aggregating multiple VPN tunnels to increase performance and provide redundancy over multiple links. See <a href="#">IPsec aggregate for redundancy and traffic load-balancing on page 1262</a> .
Redundant VPN	Options for supporting redundant and partially redundant IPsec VPNs, using route-based approaches. See <a href="#">Redundant hub and spoke VPN on page 1277</a> .
L2TP over IPsec	Configure VPN for Microsoft Windows dialup clients using the built in L2TP software. Users do not have to install any Fortinet software. See <a href="#">L2TP over IPsec on page 1226</a> .
GRE over IPsec	Legacy support for routers requiring point-to-point GRE over IPsec for tunneling. See <a href="#">GRE over IPsec on page 1160</a> .

## Phase 1 configuration

Phase 1 configuration primarily defines the parameters used in IKE (Internet Key Exchange) negotiation between the ends of the IPsec tunnel. The local end is the FortiGate interface that initiates the IKE negotiations. The remote end is the remote gateway that responds and exchanges messages with the initiator. Hence, they are sometimes referred to as the initiator and responder. The purpose of phase 1 is to secure a tunnel with one bi-directional IKE SA (security association) for negotiating IKE phase 2 parameters.

The `auto-negotiate` and `negotiation-timeout` commands control how the IKE negotiation is processed when there is no traffic, and the length of time that the FortiGate waits for negotiations to occur.

IPsec tunnels can be configured in the GUI using the *VPN Creation Wizard*. Go to *VPN > IPsec Wizard*. The wizard includes several templates (site-to-site, hub and spoke, remote access), but a custom tunnel can be configured with the following settings:

<b>Name</b>	<p>Phase 1 definition name.</p> <p>The maximum length is 15 characters for an interface mode VPN and 35 characters for a policy-based VPN.</p> <p>For a policy-based VPN, the name normally reflects where the remote connection originates. For a route-based tunnel, the FortiGate also uses the name for the virtual IPsec interface that it creates automatically.</p>
<b>Network</b>	
<b>IP Version</b>	Protocol, either IPv4 or IPv6.
<b>Remote Gateway</b>	<p>Category of the remote connection:</p> <ul style="list-style-type: none"> <li>• <i>Static IP Address</i>: the remote peer has a static IP address.</li> <li>• <i>Dialup User</i>: one or more FortiClient or FortiGate dialup clients with dynamic IP addresses will connect to the FortiGate.</li> <li>• <i>Dynamic DNS</i>: a remote peer that has a domain name and subscribes to a dynamic DNS service will connect to the FortiGate.</li> </ul>
<b>IP Address</b>	The IP address of the remote peer. This option is only available when the <i>Remote Gateway</i> is <i>Static IP Address</i> .
<b>Dynamic DNS</b>	The domain name of the remote peer. This option is only available when the <i>Remote Gateway</i> is <i>Dynamic DNS</i> .
<b>Interface</b>	<p>The interface through which remote peers or dialup clients connect to the FortiGate. This option is only available in NAT mode.</p> <p>By default, the local VPN gateway IP address is the IP address of the interface that was selected (<i>Primary IP</i> in the <i>Local Gateway</i> field).</p>
<b>Local Gateway</b>	<p>IP address for the local end of the VPN tunnel (<i>Primary IP</i> is used by default):</p> <ul style="list-style-type: none"> <li>• <i>Secondary IP</i>: secondary address of the interface selected in the <i>Interface</i> field.</li> <li>• <i>Specify</i>: manually enter an address.</li> </ul> <p>Interface mode cannot be configured in a transparent mode VDOM.</p>
<b>Mode Config</b>	<p>This option is only available when the <i>Remote Gateway</i> is <i>Dialup User</i>.</p> <p>Configure the client IP address range, subnet mask/prefix length, DNS server, and split tunnel capability to automate remote client addressing.</p>
<b>NAT Traversal</b>	<p>This option is only available when the <i>Remote Gateway</i> is <i>Static IP Address</i> or <i>Dynamic DNS</i>.</p> <p>ESP (encapsulating security payload), the protocol for encrypting data in the VPN session, uses IP protocol 50 by default. However, it does not use any port numbers so when traversing a NAT device, the packets cannot be demultiplexed. Enabling NAT traversal encapsulates the ESP packet inside a UDP packet, thereby adding a unique source port to the packet. This allows the NAT device to map the packets to the correct session.</p> <ul style="list-style-type: none"> <li>• <i>Enable</i>: a NAT device exists between the local FortiGate and the VPN</li> </ul>

	<p>peer or client. Outbound encrypted packets are wrapped inside a UDP IP header that contains a port number. The local FortiGate and the VPN peer or client must have the same NAT traversal setting (both selected or both cleared) to connect reliably. When in doubt, enable NAT traversal.</p> <ul style="list-style-type: none"> <li>• <i>Disable</i>: disable the NAT traversal setting.</li> <li>• <i>Forced</i>: the FortiGate will use a port value of zero when constructing the NAT discovery hash for the peer. This causes the peer to think it is behind a NAT device, and it will use UDP encapsulation for IPsec, even if no NAT is present. This approach maintains interoperability with any IPsec implementation that supports the NAT-T RFC.</li> </ul>
<b>Keepalive Frequency</b>	<p>Keepalive frequency setting. This option is only available when <i>NAT Traversal</i> is set to <i>Enable</i> or <i>Forced</i>. The NAT device between the VPN peers may remove the session when the VPN connection remains idle for too long.</p> <p>The value represents an interval in seconds where the connection will be maintained with periodic keepalive packets. The keepalive interval must be smaller than the session lifetime value used by the NAT device.</p> <p>The keepalive packet is a 138-byte ISAKMP exchange.</p>
<b>Dead Peer Detection</b>	<p>Reestablishes VPN tunnels on idle connections and cleans up dead IKE peers if required. This feature minimizes the traffic required to check if a VPN peer is available or unavailable (dead). The available options are:</p> <ul style="list-style-type: none"> <li>• <i>Disable</i>: disable dead peer detection (DPD).</li> <li>• <i>On Idle</i>: triggers DPD when IPsec is idle.</li> <li>• <i>On Demand</i>: Passively sends DPD to reduce load on the firewall. Only triggers DPD when IPsec outbound packets are sent, but no reply is received from the peer. When there is no traffic and the last DPD-ACK has been received, IKE will not send DPDs periodically.</li> </ul> <p>Notifications are received whenever a tunnel goes up or down, or to keep the tunnel connection open when no traffic is being generated inside the tunnel. For example, in scenarios where a dialup client or dynamic DNS peer connects from an IP address that changes periodically, traffic may be suspended while the IP address changes.</p> <p>When <i>Dead Peer Detection</i> is selected, optionally specify a retry count and a retry interval using <code>dpd-retrycount</code> and <code>dpd-retryinterval</code>. See <a href="#">Dead peer detection on page 1122</a>.</p>
<b>Forward Error Correction</b>	<p>Enable on both ends of the tunnel to correct errors in data transmission by sending redundant data across the VPN.</p>
<b>Device creation</b>	<p>Advanced option. When enabled, a dynamic interface (network device) is created for each dialup tunnel. See <a href="#">Dynamic tunnel interface creation on page 1128</a>.</p>
<b>Aggregate member</b>	<p>Advanced option. When enabled, the tunnel can be used as an aggregate member candidate.</p>
<b>Authentication</b>	

<b>Method</b>	Either <i>Pre-shared Key</i> or <i>Signature</i> .
<b>Pre-shared Key</b>	The pre-shared key that the FortiGate will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. The same key must be defined at the remote peer or client. See <a href="#">Pre-shared key</a> .
<b>Certificate Name</b>	The server certificate that the FortiGate will use to authenticate itself to the remote peer or dialup client during phase 1 negotiations. See <a href="#">Digital certificates</a> .
<b>IKE Version</b>	Either 1 or 2. See <a href="#">Choosing IKE version 1 and 2 on page 1123</a> .
<b>Mode</b>	<p>This option is only available when IKEv1 is selected. The two available options are:</p> <ul style="list-style-type: none"> <li>• <i>Aggressive</i>: the phase 1 parameters are exchanged in a single message with unencrypted authentication information.</li> <li>• <i>Main (ID protection)</i>: the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information.</li> </ul> <p>When the remote VPN peer has a dynamic IP address and is authenticated by a pre-shared key, you must select <i>Aggressive</i> mode if there is more than one dialup phase 1 configuration for the interface IP address.</p> <p>When the remote VPN peer has a dynamic IP address and is authenticated by a certificate, you must select <i>Aggressive</i> mode if there is more than one phase 1 configuration for the interface IP address and these phase 1 configurations use different proposals.</p>
<b>Peer Options</b>	Options to authenticate VPN peers or clients depending on the <i>Remote Gateway</i> and <i>Authentication Method</i> settings.
<b>Any peer ID</b>	<p>Accepts the local ID of any remote VPN peer or client. The FortiGate does not check identifiers (local IDs). <i>Mode</i> can be set to <i>Aggressive</i> or <i>Main</i>.</p> <p>This option can be used with digital certificate authentication, but for higher security, use <i>Peer certificate</i>.</p>
<b>Specific peer ID</b>	<p>This option is only available when <i>Aggressive Mode</i> is enabled. Enter the identifier that is used to authenticate the remote peer. The identifier must match the local ID configured by the remote peer's administrator.</p> <p>If the remote peer is a FortiGate, the identifier is specified in the <i>Local ID</i> field of the <i>Phase 1 Proposal</i> settings.</p> <p>If the remote peer is a FortiClient user, the identifier is specified in the <i>Local ID</i> field.</p> <p>In circumstances where multiple remote dialup VPN tunnels exist, each tunnel must have a peer ID set.</p>
<b>Peer certificate</b>	<p>Define the CA certificate used to authenticate the remote peer when the authentication mode is <i>Signature</i>.</p> <p>If the FortiGate will act as a VPN client, and you are using security certificates for authentication, set the <i>Local ID</i> to the distinguished name (DN) of the local server certificate that the FortiGate unit will use for authentication purposes.</p>

<b>Peer ID from dialup group</b>	<p>Authenticate multiple FortiGate or FortiClient dialup clients that use unique identifiers and unique pre-shared keys (or unique pre-shared keys only) through the same VPN tunnel.</p> <p>You must create a dialup user group for authentication purposes. Select the group from the list next to the <i>Peer ID from dialup group</i> option.</p> <p>You must set <i>Mode</i> to <i>Aggressive</i> when the dialup clients use unique identifiers and unique pre-shared keys. If the dialup clients use unique pre-shared keys only, you can set <i>Mode</i> to <i>Main</i> if there is only one dialup Phase 1 configuration for this interface IP address.</p>
<b>Phase 1 Proposal</b>	<p>The encryption and authentication algorithms used to generate keys for the IKE SA.</p> <p>There must be a minimum of one combination. The remote peer or client must be configured to use at least one of the proposals that you define.</p>
<b>Encryption</b>	<p>The following symmetric-key encryption algorithms are available:</p> <ul style="list-style-type: none"> <li>• <i>DES</i>: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.</li> <li>• <i>3DES</i>: triple-DES; plain text is encrypted three times by three keys.</li> <li>• <i>AES128</i>: Advanced Encryption Standard, a 128-bit block algorithm that uses a 128-bit key.</li> <li>• <i>AES128GCM</i>: AES in Galois/Counter Mode, a 128-bit block algorithm that uses a 128-bit key. Only available for IKEv2.</li> <li>• <i>AES192</i>: a 128-bit block algorithm that uses a 192-bit key.</li> <li>• <i>AES256</i>: a 128-bit block algorithm that uses a 256-bit key.</li> <li>• <i>AES256GCM</i>: AES in Galois/Counter Mode, a 128-bit block algorithm that uses a 256-bit key. Only available for IKEv2.</li> <li>• <i>CHACHA20POLY1305</i>: a 128-bit block algorithm that uses a 128-bit key and a symmetric cipher. Only available for IKEv2. See also <a href="#">HMAC settings</a>.</li> </ul>
<b>Authentication</b>	<p>The following message digests that check the message authenticity during an encrypted session are available:</p> <ul style="list-style-type: none"> <li>• <i>MD5</i>: message digest 5.</li> <li>• <i>SHA1</i>: secure hash algorithm 1; a 160-bit message digest.</li> <li>• <i>SHA256</i>: a 256-bit message digest.</li> <li>• <i>SHA384</i>: a 384-bit message digest.</li> <li>• <i>SHA512</i>: a 512-bit message digest.</li> </ul> <p>In IKEv2, encryption algorithms include authentication, but a PRF (pseudo random function) is still required (<i>PRFSHA1</i>, <i>PRFSHA256</i>, <i>PRFSHA384</i>, <i>PRFSHA512</i>). See also <a href="#">HMAC settings</a>.</p>
<b>Diffie-Hellman Groups</b>	<p>Asymmetric key algorithms used for public key cryptography.</p> <p>Select one or more from groups 1, 2, 5, and 14 through 32. At least one of the <i>Diffie-Hellman Groups</i> (DH) settings on the remote peer or client must match one the selections on the FortiGate. Failure to match one or more DH groups will result in failed negotiations.</p>

<b>Key Lifetime</b>	The time (in seconds) that must pass before the IKE encryption key expires. When the key expires, a new key is generated without interrupting service. The keylife can be from 120 to 172 800 seconds.
<b>Local ID</b>	Optional setting. This value must match the peer ID value given for the remote VPN peer's <i>Peer Options</i> . <ul style="list-style-type: none"> <li>If the FortiGate will act as a VPN client and you are using peer IDs for authentication purposes, enter the identifier that the FortiGate will supply to the VPN server during the phase 1 exchange.</li> <li>If the FortiGate will act as a VPN client and you are using security certificates for authentication, select the distinguished name (DN) of the local server certificate that the FortiGate will use for authentication purposes.</li> </ul>
<b>XAUTH</b>	This option supports the authentication of dialup clients. It is only available for IKE version 1. <ul style="list-style-type: none"> <li><i>Disable</i>: do not use XAuth.</li> <li><i>Client</i>: available only if the <i>Remote Gateway</i> is set to <i>Static IP Address</i> or <i>Dynamic DNS</i>. If the FortiGate is a dialup client, enter the user name and password for the FortiGate to authenticate itself to the remote XAuth server.</li> <li><i>PAP Server, CHAP Server, Auto Server</i>: available only if <i>Remote Gateway</i> is set to <i>Dialup User</i>. Dialup clients authenticate as members of a dialup user group. A user group must be created first for the dialup clients that need access to the network behind the FortiGate.</li> </ul> <p>The FortiGate must be configured to forward authentication requests to an external RADIUS or LDAP authentication server.</p> <p>Select the server type based on the encryption method used between the FortiGate, the XAuth client, and the external authentication server. Then select the user group (<i>Inherit from policy</i> or <i>Choose</i>). See <a href="#">Using XAuth authentication on page 1126</a>.</p>
<b>Username</b>	User name used for authentication.
<b>Password</b>	Password used for authentication.

## Additional CLI configurations

The following phase 1 settings can be configured in the CLI:

<b>VXLAN over IPsec</b>	Packets with a VXLAN header are encapsulated within IPsec tunnel mode.
<b>To configure VXLAN over IPsec:</b> <pre> config vpn ipsec phase1-interface/phase1     edit ipsec         set interface &lt;name&gt;         set encapsulation vxlan/gre         set encapsulation-address ike/ipv4/ipv6         set encaps-local-gw4 xxx.xxx.xxx.xxx </pre>	

```

 set encaps-remote-gw xxx.xxx.xxx.xxx
 next
end

```

**IPsec tunnel idle timer**

Define an idle timer for IPsec tunnels. When no traffic has passed through the tunnel for the configured `idle-timeout` value, the IPsec tunnel will be flushed.

**To configure IPsec tunnel idle timeout:**

```

config vpn ipsec phase1-interface
 edit p1
 set idle-timeout {enable | disable}
 set idle-timeoutinterval <integer> IPsec tunnel idle
 timeout in minutes (10 - 43200).
 next
end

```

**Monitor tunnel for failover**

Monitor a site-to-site tunnel to guarantee operational continuity if the primary tunnel fails. Configure the secondary phase 1 interface to monitor the primary interface.

**To configure the monitor:**

```

config vpn ipsec phase1-interface
 edit <secondary phase1-interface>
 set monitor <primary phase1-interface>
 next
end

```

**Passive mode**

Passive mode turns one side of the tunnel to be a responder only. It does not initiate VPN tunnels either by auto-negotiation, rekey, or traffic initiated behind the FortiGate.

**To configure passive mode:**

```

config vpn ipsec phase1-interface
 edit <example>
 set rekey {enable | disable}
 set passive-mode {enable | disable}
 set passive-tunnel-interface {enable | disable}
 next
end

```

**Network ID**

The network ID is a Fortinet-proprietary attribute that is used to select the correct phase 1 between IPsec peers, so that multiple IKEv2 tunnels can be established between the same local/remote gateway pairs.

In a dial-up VPN, `network-id` is in the first initiator message of an IKEv2 phase 1 negotiation. The responder (Hub) uses the `network-id` to match a phase 1 configuration with a matching `network-id`. The Hub can then differentiate multiple dial-up phase 1s that are bound to the same underlay interface and IP address. Without a `network-id`, the Hub cannot have multiple phase 1 dialup tunnels on the same interface.

In static phase 1 configurations, `network-id` is used with the pair of gateway IPs to negotiate the correct tunnel with a matching `network-id`. This allows IPsec peers to use the same pair of underlay IPs to establish multiple IPsec tunnels. Without it, only a single tunnel can be established over the same pair of underlay IPs.

#### To configure the network ID:

```
config vpn ipsec phase1-interface
 edit <example>
 set network-id <integer>
 next
end
```

## Dead peer detection

By default, dead peer detection (DPD) sends probe messages every five seconds. If you are experiencing high network traffic, you can experiment with increasing the ping interval. However, longer intervals will require more traffic to detect dead peers, which will result in more traffic.



In a dynamic (dialup) connection, the *On Idle* option encourages dialup server configurations to more proactively delete tunnels if the peer is unavailable.

In the GUI, the dead peer detection option can be configured when defining phase 1 options. The following CLI commands support additional options for specifying a retry count and a retry interval.

For example, enter the following to configure DPD on the existing IPsec phase 1 configuration to use 15-second intervals and to wait for three missed attempts before declaring the peer dead and taking action.

#### To configure DPD:

```
config vpn ipsec phase1-interface
 edit <value>
 set dpd [disable | on-idle | on-demand]
 set dpd-retryinterval 15
 set dpd-retrycount 3
 next
end
```

## DPD scalability

On a dialup server, if many VPN connections are idle, the increased DPD exchange could negatively impact the performance/load of the daemon. The *on-demand* option in the CLI triggers DPD when IPsec traffic is sent, but no reply



is received from the peer.

When there is no traffic and the last DPD-ACK had been received, IKE will not send DPDs periodically. IKE will only send out DPDs if there are outgoing packets to send, but no inbound packets have since been received.

## HMAC settings

The FortiGate uses the HMAC based on the authentication proposal that is chosen in phase 1 or phase 2 of the IPsec configuration. Each proposal consists of the encryption-hash pair (such as `3des-sha256`). The FortiGate matches the most secure proposal to negotiate with the peer.

### To view the chosen proposal and the HMAC hash used:

```
diagnose vpn ike gateway list

vd: root/0
name: MPLS
version: 1
interface: port1 3
addr: 192.168.2.5:500 -> 10.10.10.1:500
virtual-interface-addr: 172.31.0.2 -> 172.31.0.1
created: 1015820s ago
IKE SA: created 1/13 established 1/13 time 10/1626/21010 ms
IPsec SA: created 1/24 established 1/24 time 0/11/30 ms

id/spi: 124 43b087dae99f7733/6a8473e58cd8990a
direction: responder
status: established 68693-68693s ago = 10ms
proposal: 3des-sha256
key: e0fa6ab8dc509b33-aa2cc549999b1823-c3cb9c337432646e
lifetime/rekey: 86400/17436
DPD sent/recv: 000001e1/00000000
```

## Choosing IKE version 1 and 2

If you create a route-based VPN, you have the option of selecting IKE version 2. Otherwise, IKE version 1 is used.

IKEv2, defined in [RFC 4306](#), simplifies the negotiation process that creates the security association (SA).

If you select IKEv2:

- There is no choice in phase 1 of aggressive or main mode.
- Extended authentication (XAUTH) is not available.
- You can utilize EAP and MOBIKE.

### Repeated authentication in IKEv2

This feature provides the option to control whether a device requires its peer to re-authenticate or whether re-key is sufficient. It does not influence the re-authentication or re-key behavior of the device itself, which is controlled by the peer (the default being to re-key). This solution is in response to [RFC 4478](#). As described by the IETF, "the purpose of this is to limit the time that security associations (SAs) can be used by a third party who has gained control of the IPsec peer".

To configure IKE SA re-authentication:

```
config vpn ipsec phase1-interface
 edit p1
 set reauth [enable | disable]
 next
end
```

### **IKEv2 quick crash detection**

There is support for IKEv2 quick crash detection (QCD) as described in [RFC 6290](#).

RFC 6290 describes a method in which an IKE peer can quickly detect that the gateway peer it has and established an IKE session with has rebooted, crashed, or otherwise lost IKE state. When the gateway receives IKE messages or ESP packets with unknown IKE or IPsec SPIs, the IKEv2 protocol allows the gateway to send the peer an unprotected IKE message containing INVALID\_IKE\_SPI or INVALID\_SPI notification payloads.

RFC 6290 introduces the concept of a QCD token, which is generated from the IKE SPIs and a private QCD secret, and exchanged between peers during the protected IKE AUTH exchange.

#### **To configure QCD:**

```
config system settings
 set ike-quick-crash-detect [enable | disable]
end
```

### **IKEv1 quick crash detection**

Based on the IKEv2 QCD feature previously described, IKEv1 QCD is implemented using a new IKE vendor ID (Fortinet Quick Crash Detection) so both endpoints must be FortiGates. The QCD token is sent in the phase 1 exchange and must be encrypted, so this is only implemented for IKEv1 in main mode (aggressive mode is not supported as there is no available AUTH message to include the token). Otherwise, the feature works the same as in IKEv2 (RFC 6290).

### **IKEv1 fragmentation**

UDP fragmentation can cause issues in IPsec when either the ISP or perimeter firewall(s) cannot pass or fragment the oversized UDP packets that occur when using a very large public security key (PSK). The result is that IPsec tunnels do not come up. The solution is IKE fragmentation.

For most configurations, enabling IKE fragmentation allows connections to automatically establish when they otherwise might have failed due to intermediate nodes dropping IKE messages containing large certificates, which typically push the packet size over 1500 bytes.

FortiOS will fragment a packet on sending if only all the following are true:

- Phase 1 contains `set fragmentation enable`.
- The packet is larger than the minimum MTU (576 for IPv4, 1280 for IPv6).
- The packet is being re-transmitted.

By default, IKE fragmentation is enabled.

#### **To configure IKEv1 fragmentation:**

```
config vpn ipsec phase1-interface
 edit 1
 set fragmentation [enable | disable]
```

```
 next
end
```

## IKEv2 fragmentation

[RFC 7383](#) requires each fragment to be individually encrypted and authenticated. With IKEv2, a copy of the unencrypted payloads around for each outgoing packet would need to be kept in case the original single packet was never answered and would retry with fragments. With the following implementation, if the IKE payloads are greater than a configured threshold, the IKE packets are preemptively fragmented and encrypted.

### To configure IKEv2 fragmentation:

```
config vpn ipsec phase1-interface
 edit ike
 set ike-version 2
 set fragmentation [enable|disable]
 set fragmentation-mtu [500-16000]
 next
end
```

## Pre-shared key vs digital certificates

A FortiGate can authenticate itself to remote peers or dialup clients using either a pre-shared key or a digital certificate.

### Pre-shared key

Using a pre-shared key is less secure than using certificates, especially if it is used alone, without requiring peer IDs or extended authentication (XAuth). There also needs to be a secure way to distribute the pre-shared key to the peers.

If you use pre-shared key authentication alone, all remote peers and dialup clients must be configured with the same pre-shared key. Optionally, you can configure remote peers and dialup clients with unique pre-shared keys. On the FortiGate, these are configured in user accounts, not in the phase 1 settings.

The pre-shared key must contain at least six printable characters and should be known by network administrators. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters. The limit is 128 characters.

If you authenticate the FortiGate using a pre-shared key, you can require remote peers or dialup clients to authenticate using peer IDs, but not client certificates.

### To authenticate the FortiGate using a pre-shared key:

1. Go to *VPN > IPsec Tunnels* and create a new tunnel, or edit an existing one.
2. Configure or edit the *Network* section as needed.
3. Configure or edit the *Authentication* settings as follows:

Method	<i>Pre-shared Key</i>
<b>Pre-shared Key</b>	<string>
<b>IKE Version</b>	1 or 2
<b>Mode</b>	<i>Aggressive</i> or <i>Main</i>

**Peer Options**

Select an *Accept Type* and the corresponding peer. Options vary based on the *Remote Gateway* and *Authentication Method* settings in the *Network* section. *Peer Options* are only available in *Aggressive* mode.

4. For the *Phase 1 Proposal* section, keep the default settings unless changes are needed to meet your requirements.
5. Optionally, for authentication parameters for a dialup user group, define *XAUTH* parameters.
6. Click *OK*.

**Digital certificates**

To authenticate the FortiGate using digital certificates, you must have the required certificates installed on the remote peer and on the FortiGate. The signed server certificate on one peer is validated by the presence of the root certificate installed on the other peer. If you use certificates to authenticate the FortiGate, you can also require the remote peers or dialup clients to authenticate using certificates. See [Site-to-site VPN with digital certificate on page 1145](#) for a detailed example.

**To authenticate the FortiGate using a digital certificate:**

1. Go to *VPN > IPsec Tunnels* and create a new tunnel, or edit an existing one.
2. Configure or edit the *Network* section as needed.
3. Configure or edit the *Authentication* settings as follows:

Method	Signature
<b>Certificate Name</b>	Select the certificate used to identify this FortiGate. If there are no imported certificates, use <i>Fortinet_Factory</i> .
<b>IKE Version</b>	1 or 2
<b>Mode</b>	<i>Aggressive</i> is recommended.
<b>Peer Options</b>	For <i>Accept Type</i> , select <i>Peer certificate</i> and select the peer and the CA certificate used to authenticate the peer. If the other end is using the Fortinet_Factory certificate, then use the <i>Fortinet_CA</i> certificate here.

4. For the *Phase 1 Proposal* section, keep the default settings unless changes are needed to meet your requirements.
5. Optionally, for authentication parameters for a dialup user group, define *XAUTH* parameters.
6. Click *OK*.

**Using XAuth authentication**

Extended authentication (XAuth) increases security by requiring remote dialup client users to authenticate in a separate exchange at the end of phase 1. XAuth draws on existing FortiGate user group definitions and uses established authentication mechanisms such as PAP, CHAP, RADIUS, and LDAP to authenticate dialup clients. You can configure a FortiGate to function either as an XAuth server or client. If the server or client is attempting a connection using XAuth and the other end is not using XAuth, the failed connection attempts that are logged will not specify XAuth as the reason.

**XAuth server**

A FortiGate can act as an XAuth server for dialup clients. When the phase 1 negotiation completes, the FortiGate challenges the user for a user name and password. It then forwards the user's credentials to an external RADIUS or LDAP server for verification.

If the user records on the RADIUS server have suitably configured Framed-IP-Address fields, you can assign client virtual IP addresses by XAuth instead of from a DHCP address range.

The authentication protocol you use for XAuth depends on the capabilities of the authentication server and the XAuth client:

- Select *PAP Server* whenever possible.
- You must select *PAP Server* for all implementations of LDAP and some implementations of Microsoft RADIUS.
- Select *Auto Server* when the authentication server supports *CHAP Server* but the XAuth client does not. The FortiGate will use PAP to communicate with the XAuth client and CHAP to communicate with the authentication server. You can also use *Auto Server* to allow multiple source interfaces to be defined in an IPsec/IKE policy.

Before you begin, create user accounts and user groups to identify the dialup clients that need to access the network behind the FortiGate dialup server. If password protection will be provided through an external RADIUS or LDAP server, you must configure the FortiGate dialup server to forward authentication requests to the authentication server.

### To configure XAuth to authenticate a dialup user group:

1. On the FortiGate dialup server, go to *VPN > IPsec Tunnels* and create a new tunnel, or edit an existing one.
2. Configure or edit the *Network*, *Authentication*, and *Phase 1 Proposal* sections as needed.
3. In the *XAUTH* section, select the encryption method *Type* to use between the XAuth client, the FortiGate, and the authentication server.
4. For *User Group*:
  - a. Click *Inherit from policy* for multiple user groups defined in the IPsec/IKE policy, or
  - b. Click *Choose* and in the dropdown, select the user group that needs to access the private network behind the FortiGate.



Only one user group may be defined for *Auto Server*.

---

5. Click *OK*.
6. Create as many policies as needed, specifying the source user(s) and destination address.

### XAuth client

If the FortiGate acts as a dialup client, the remote peer, acting as an XAuth server, might require a username and password. You can configure the FortiGate as an XAuth client with its own username and password, which it provides when challenged.

### To configure the FortiGate dialup client as an XAuth client:

1. On the FortiGate dialup client, go to *VPN > IPsec Tunnels* and create a new tunnel, or edit an existing one.
2. Configure or edit the *Network*, *Authentication*, and *Phase 1 Proposal* sections as needed.
3. In the *XAUTH* section, for *Type*, select *Client*.
4. For *Username*, enter the FortiGate PAP, CHAP, RADIUS, or LDAP user name that the FortiGate XAuth server will compare to its records when the FortiGate XAuth client attempts to connect.
5. Enter the *Password* for the user name.
6. Click *OK*.

## Dynamic IPsec route control

You can add a route to a peer destination selector by using the `add-route` option, which is available for all dynamic IPsec phases 1 and 2, for both policy-based and route-based IPsec VPNs.

The `add-route` option adds a route to the FortiGate routing information base when the dynamic tunnel is negotiated. You can use the `distance` and `priority` options to set the distance and priority of this route. If this results in a route with the lowest distance, it is added to the FortiGate forwarding information base.

You can also enable `add-route` in any policy-based or route-based phase 2 configuration that is associated with a dynamic (dialup) phase 1. In phase 2, `add-route` can be enabled, disabled, or set to use the same route as phase 1.

The `add-route` option is enabled by default.

### To configure add-route in phase 1:

```
config vpn ipsec
 edit <name>
 set type dynamic
 set add-route {enable | disable}
 next
end
```

### To configure add-route in phase 2:

```
config vpn ipsec {phase2 | phase2-interface}
 edit <name>
 set add-route {phase1 | enable | disable}
 next
end
```

## Blocking IPsec SA negotiation

For interface-based IPsec, IPsec SA negotiation blocking can only be removed if the peer offers a wildcard selector. If a wildcard selector is offered, then the wildcard route will be added to the routing table with the distance/priority value configured in phase 1. If that is the route with the lowest distance, it will be installed into the forwarding information base.

In this scenario, it is important to ensure that the distance value configured for phase 1 is set appropriately.

## Dynamic tunnel interface creation

When configuring route-based IPsec dialup tunnels, the `net-device` setting controls how traffic is routed on the hub:

```
config vpn ipsec phase1-interface
 edit "Spoke"
 set type dynamic
 set net-device {disable | enable}
 set tunnel-search {selectors | nexthop}
 next
end
```

The key settings are `net-device` and `tunnel-search`. When `net-device` is disabled, all dialup tunnels share an interface on the hub. The tunnel selection process is based on the tunnel search method. Using a shared interface eliminates the time needed for dynamic interface creation and tear-down. When `net-device` is enabled, dynamic

interfaces are created on the hub for each dialup tunnel. This means that potentially many dynamic interfaces could be created at start-up in a large scale deployment.

### Behavior with net-device disabled

After a successful dial-in negotiation, the following occurs on the hub:

1. A dialup tunnel is created for each successful dial-in.
2. The tunnel name takes the form of <phase1Name\_index>.
  - a. For example, the first dialup tunnel to connect is Spoke\_1, the second is Spoke\_2, and so on.

To view the tunnel name and the phase 1 parent:

```
Hub # diagnose vpn tunnel list name Spoke_3
list ipsec tunnel by names in vd 0

name=Spoke_3 ver=1 serial=8 198.51.100.1:0->198.51.100.4:0
bound_if=4 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/320 options
[0140]=search-nexthop rgwy_chg parent=Spoke index=3
```

3. No dynamic interface is created.
4. The networks accessible over dialup tunnels are all bound to the same shared phase 1 interface.
  - a. To view the routing table:

```
Hub # get router info routing-table bgp
Routing table for VRF=0
B 192.168.2.0/24 [200/0] via 10.10.10.2, Spoke, 01:04:49
B 192.168.3.0/24 [200/0] via 10.10.10.3, Spoke, 01:04:47
B 192.168.4.0/24 [200/0] via 10.10.10.4, Spoke, 00:35:01
B 192.168.5.0/24 [200/0] via 10.10.10.5, Spoke, 01:04:51
```

When forwarding a packet to the spoke shared interface:

1. The cleartext packet is first sent to the IPsec engine.
2. The IPsec engine finds which tunnel's IPsec security association (SA) is used for protecting this packet.
3. The search logic is based on `set tunnel-search {selectors | nexthop}`.

### Tunnel search selectors

This is the default setting, which dictates that IPsec routes are learned from the traffic selectors of the IPsec SA negotiation. These routes are also called IKE routes, and can be displayed using `diagnose vpn ike routes list`.

### Tunnel search next hop

This setting is used when you want IPsec routes to be learned from a dynamic routing protocol. The IPsec engine checks the search method associated with the shared interface spoke, and searches the tunnel index associated with the next hop. In this example, while searching for the index associated with next hop 10.10.10.4, index 3 is found corresponding to the Spoke\_3 tunnel.

```
Hub # diagnose vpn tunnel list name Spoke
list ipsec tunnel by names in vd 0

name=Spoke ver=1 serial=1 198.51.100.1:0->0.0.0.0:0
bound_if=4 lgwy=static/1 tun=intf/0 mode=dialup/2 encap=none/64 options[0040]=search-nexthop
proxyid_num=0 child_num=4 refcnt=26 ilast=4159 olast=4159 ad=/0 itn-status=7b
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
```

```
run_tally=4
ipv4 route tree:
10.10.10.2 2
10.10.10.3 0
10.10.10.4 3
10.10.10.5 1
198.51.100.2 2
198.51.100.3 0
198.51.100.4 3
198.51.100.5 1
```

## Behavior with net-device enabled

After a successful dial-in negotiation, the following occurs on the hub:

1. A dialup tunnel is created for each successful dial-in.
2. The tunnel name takes the form of <phase1Name\_index>.
  - a. For example, the first dialup tunnel to connect is Spoke\_1, the second is Spoke\_2, and so on.

To view the tunnel name and the phase 1 parent:

```
Hub # diagnose vpn tunnel list name Spoke_3
list ipsec tunnel by names in vd 0

name=Spoke_3 ver=1 serial=6 198.51.100.1:0->198.51.100.4:0
bound_if=4 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/0 parent=Spoke
index=3
```

3. A dynamic interface is created for each dialup tunnel.

- a. To view the interface list:

```
Hub # diagnose netlink interface list | grep "Spoke_"
if=Spoke_0 family=00 type=768 index=22 mtu=1438 link=16 master=0
if=Spoke_1 family=00 type=768 index=23 mtu=1438 link=16 master=0
if=Spoke_2 family=00 type=768 index=24 mtu=1438 link=16 master=0
if=Spoke_3 family=00 type=768 index=26 mtu=1438 link=16 master=0
```

4. The networks accessible over dialup tunnels are bound to the corresponding tunnel interface.

- a. To view the routing table:

```
Hub # get router info routing-table bgp
Routing table for VRF=0
B 192.168.2.0/24 [200/0] via 10.10.10.2, Spoke_0, 01:04:49
B 192.168.3.0/24 [200/0] via 10.10.10.3, Spoke_1, 01:04:47
B 192.168.4.0/24 [200/0] via 10.10.10.4, Spoke_3, 00:35:01
B 192.168.5.0/24 [200/0] via 10.10.10.5, Spoke_2, 01:04:51
```

When forwarding a packet to the dialup IPsec interface:

1. The cleartext packet sent to the dynamic interface is sent to the IPsec engine.
2. The IPsec engine protects the cleartext packets with the IPsec security association (SA) of the corresponding tunnel.
3. The ESP packet is then sent on the wire.



## Phase 2 configuration

After phase 1 negotiations end successfully, phase 2 begins. In Phase 2, the VPN peer or client and the FortiGate exchange keys again to establish a secure communication channel. The phase 2 proposal parameters select the encryption and authentication algorithms needed to generate keys for protecting the implementation details of security associations (SAs). The keys are generated automatically using a Diffie-Hellman algorithm.

The basic phase 2 settings associate IPsec phase 2 parameters with the phase 1 configuration that specifies the remote end point of the VPN tunnel. In most cases, you need to configure only basic Phase 2 settings.

Some settings can be configured in the CLI. The following options are available in the *VPN Creation Wizard* after the tunnel is created:

New Phase 2	
<b>Name</b>	Phase 2 definition name.
<b>Local Address</b>	<p>A value of 0.0.0.0/0 means all IP addresses behind the local VPN peer. Add a specific address or range to allow traffic from and to only this local address.</p> <p>See <a href="#">Quick mode selectors on page 1133</a>.</p>
<b>Remote Address</b>	<p>Enter the destination IP address that corresponds to the recipients or network behind the remote VPN peer. A value of 0.0.0.0/0 means all IP addresses behind the remote VPN peer.</p> <p>See <a href="#">Quick mode selectors on page 1133</a>.</p>
<b>Advanced</b>	Select the encryption and authentication algorithms that will be proposed to the remote VPN peer. To establish a VPN connection, at least one of the proposals specified must match the configuration on the remote peer.
<b>Encryption</b>	<p>The following symmetric-key encryption algorithms are available:</p> <ul style="list-style-type: none"> <li><b>NULL</b>: do not use an encryption algorithm.</li> <li><b>DES</b>: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.</li> <li><b>3DES</b>: triple-DES; plain text is encrypted three times by three keys.</li> <li><b>AES128</b>: Advanced Encryption Standard, a 128-bit block algorithm that uses a 128-bit key.</li> <li><b>AES128GCM</b>: AES in Galois/Counter Mode, a 128-bit block algorithm that uses a 128-bit key. Only available for IKEv2.</li> <li><b>AES192</b>: a 128-bit block algorithm that uses a 192-bit key.</li> <li><b>AES256</b>: a 128-bit block algorithm that uses a 256-bit key.</li> <li><b>AES256GCM</b>: AES in Galois/Counter Mode, a 128-bit block algorithm that uses a 256-bit key. Only available for IKEv2.</li> <li><b>CHACHA20POLY1305</b>: a 128-bit block algorithm that uses a 128-bit key and a symmetric cipher. Only available for IKEv2.</li> </ul> <p>See <a href="#">ChaCha20 and Poly1305 AEAD cipher on page 1134</a>, <a href="#">AES-GCM for IKEv2 phase 1 on page 1135</a>, and <a href="#">HMAC settings</a>.</p>
<b>Authentication</b>	<p>The following message digests that check the message authenticity during an encrypted session are available:</p> <ul style="list-style-type: none"> <li><b>NULL</b>: do not use a message digest.</li> </ul>

	<ul style="list-style-type: none"> <li>• <i>MD5</i>: message digest 5.</li> <li>• <i>SHA1</i>: secure hash algorithm 1; a 160-bit message digest.</li> <li>• <i>SHA256</i>: a 256-bit message digest.</li> <li>• <i>SHA384</i>: a 384-bit message digest.</li> <li>• <i>SHA512</i>: a 512-bit message digest.</li> </ul> <p>See also <a href="#">HMAC settings</a>.</p>
<b>Enable Replay Detection</b>	<p>Replay attacks occur when an unauthorized party intercepts a series of IPsec packets and replays them back into the tunnel.</p> <p>Replay detection allows the FortiGate to check all IPsec packets to see if they have been received before. If any encrypted packets arrive out of order, the FortiGate discards them.</p> <p>Note that 64-bit extended sequence numbers (as described in RFC 4303, RFC 4304 as an addition to IKEv1, and RFC 5996 for IKEv2) are supported for IPsec when replay detection is enabled.</p>
<b>Enable Perfect Forward Secrecy (PFS)</b>	<p>Perfect forward secrecy (PFS) improves security by forcing a new Diffie-Hellman exchange whenever keylife expires.</p>
<b>Diffie-Hellman Group</b>	<p>Asymmetric key algorithms used for public key cryptography.</p> <p>Select one or more from groups 1, 2, 5, and 14 through 32. At least one of the <i>Diffie-Hellman Groups</i> (DH) settings on the remote peer or client must match one the selections on the FortiGate. Failure to match one or more DH groups will result in failed negotiations.</p>
<b>Local Port</b>	<p>Enter the port number that the local VPN peer uses to transport traffic related to the specified service (protocol number). The range is from 0 to 65535. To specify all ports, select <i>All</i>, or enter 0.</p>
<b>Remote Port</b>	<p>Enter the port number that the remote VPN peer uses to transport traffic related to the specified service (protocol number). To specify all ports, select <i>All</i>, or enter 0.</p>
<b>Protocol</b>	<p>Enter the IP protocol number of the service. To specify all services, select <i>All</i>, or enter 0.</p>
<b>Auto-negotiate</b>	<p>Select this option for the tunnel to be automatically renegotiated when the it expires. See <a href="#">Auto-negotiate on page 1133</a>.</p>
<b>Autokey Keep Alive</b>	<p>Select this option for the tunnel to remain active when no data is being processed.</p>
<b>Key Lifetime</b>	<p>Select the method for determining when the phase 2 key expires:</p> <ul style="list-style-type: none"> <li>• <i>Seconds</i></li> <li>• <i>Kilobytes</i></li> <li>• <i>Both</i></li> </ul> <p>Enter a corresponding value for <i>Seconds</i> and/or <i>Kilobytes</i> in the text boxes. If <i>Both</i> is selected, the key expires when either the time has passed or the number of kilobytes have been processed.</p>

## Quick mode selectors

Quick mode selectors determine which IP addresses can perform IKE negotiations to establish a tunnel. By only allowing authorized IP addresses access to the VPN tunnel, the network is more secure.

The default settings are as broad as possible: any IP address or configured address object using any protocol on any port.



While the dropdown menus for specifying an address also show address groups, the use of address groups may not be supported on a remote endpoint device that is not a FortiGate.

---

When configuring a quick mode selector for *Local Address* and *Remote Address*, valid options include IPv4 and IPv6 single addresses, subnets, or ranges.

There are some configurations that require specific selectors:

- The VPN peer is a third-party device that uses specific phase2 selectors.
- The FortiGate connects as a dialup client to another FortiGate, in which case (usually) you must specify a local IP address, IP address range, or subnet. However, this is not required if you are using dynamic routing and `mode-cfg`.

With FortiOS VPNs, your network has multiple layers of security, with quick mode selectors being an important line of defense:

- Routes guide traffic from one IP address to another.
- Phase 1 and phase 2 connection settings ensure there is a valid remote end point for the VPN tunnel that agrees on the encryption and parameters.
- Quick mode selectors allow IKE negotiations only for allowed peers.
- Security policies control which IP addresses can connect to the VPN.
- Security policies also control what protocols are allowed over the VPN along with any bandwidth limiting.

If you are editing an existing phase 2 configuration, the local address and remote address fields are unavailable if the tunnel has been configured to use firewall addresses as selectors. This option exists only in the CLI.

## Using the add-route option

Consider using the `add-route` option to add a route to a peer destination selector in phase 2 to automatically match the settings in phase 1.

### To configure add-route:

```
config vpn ipsec {phase2 | phase2-interface}
 edit <name>
 set add-route {phase1 | enable | disable}
 next
end
```

## Auto-negotiate

By default, the phase 2 security association (SA) is not negotiated until a peer attempts to send data. The triggering packet and some subsequent packets are dropped until the SA is established. Applications normally resend this data, so there is no loss, but there might be a noticeable delay in response to the user.

If the tunnel goes down, the auto-negotiate feature (when enabled) attempts to re-establish the tunnel. Auto-negotiate initiates the phase 2 SA negotiation automatically, repeating every five seconds until the SA is established.

Automatically establishing the SA can be important for a dialup peer. It ensures that the VPN tunnel is available for peers at the server end to initiate traffic to the dialup peer. Otherwise, the VPN tunnel does not exist until the dialup peer initiates traffic.

### To configure auto-negotiate:

```
config vpn ipsec phase2
 edit <phase2_name>
 set auto-negotiate enable
 next
end
```

### Installing dynamic selectors via auto-negotiate

The IPsec SA connect message generated is used to install dynamic selectors. These selectors can be installed via the auto-negotiate mechanism. When phase 2 has `auto-negotiate` enabled, and phase 1 has `mesh-selector-type` set to `subnet`, a new dynamic selector will be installed for each combination of source and destination subnets. Each dynamic selector will inherit the auto-negotiate option from the template selector and begin SA negotiation. Phase 2 selector sources from dialup clients will all establish SAs without traffic being initiated from the client subnets to the hub.

## DHCP

The `dhcp-ipsec` option lets the FortiGate assign VIP addresses to FortiClient dialup clients through a DHCP server or relay. This option is only available if the remote gateway in the phase 1 configuration is set to dialup user, and it only works in policy-based VPNs.

With `dhcp-ipsec`, the FortiGate dialup server acts as a proxy for FortiClient dialup clients that have VIP addresses on the subnet of the private network behind the FortiGate. In this case, the FortiGate dialup server acts as a proxy on the local private network for the FortiClient dialup client. A host on the network behind the dialup server issues an ARP request, corresponding to the device MAC address of the FortiClient host (when a remote server sends an ARP to the local FortiClient dialup client). The FortiGate then answers the ARP request on behalf of the FortiClient host, and then forwards the associated traffic to the FortiClient host through the tunnel.

Acting as a proxy prevents the VIP address assigned to the FortiClient dialup client from causing possible ARP broadcast problems—the normal and VIP addresses can confuse some network switches when two addresses have the same MAC address.

## ChaCha20 and Poly1305 AEAD cipher

In IKEv2 to support [RFC 7634](#), the ChaCha20 and Poly1305 crypto algorithms can be used together as a combined mode AEAD cipher (like AES-GCM) in the `crypto_ftnt` cipher in `cipher_chacha20poly1305.c`:

```
config vpn ipsec phase2-interface
 edit <name>
 set phase1name <name>
 set proposal chacha20poly1305
 next
end
```

## AES-GCM for IKEv2 phase 1

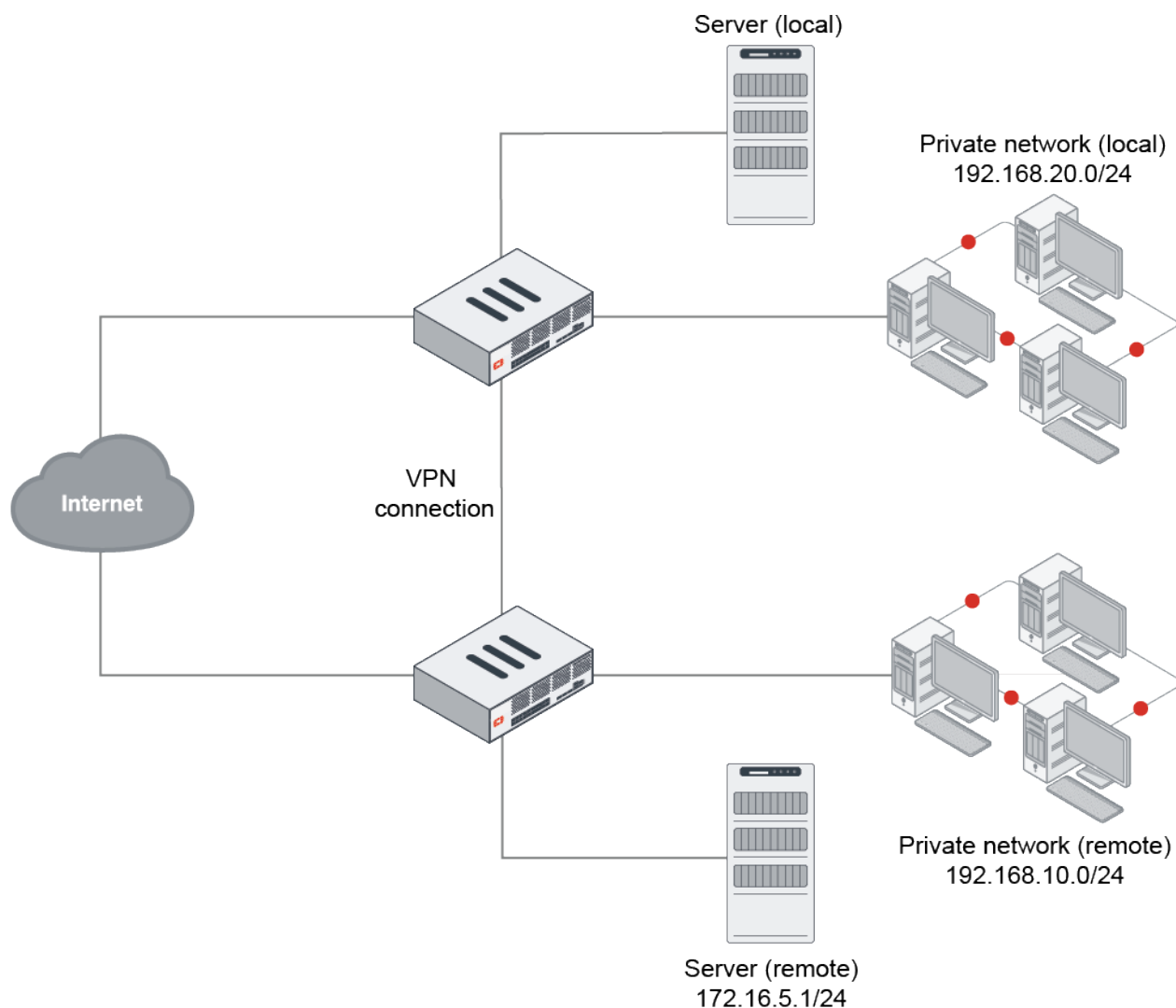
In IKEv2 to support [RFC 5282](#), the AEAD algorithm AES-GCM supports 128- and 256-bit variants:

```
config vpn ipsec phase2-interface
 edit <name>
 set phase1name <name>
 set proposal [aes128gcm | aes256gcm]
 next
end
```

## VPN security policies

This section explains how to specify the source and destination IP addresses of traffic transmitted through an IPsec VPN, and how to define appropriate security policies.

### Topology



## Defining policy addresses

In a gateway-to-gateway, hub-and-spoke, dynamic DNS, redundant tunnel, or transparent configuration, you need to define a policy address for the private IP address of the network behind the remote VPN peer (for example, 192.168.10.0/255.255.255.0 or 192.168.10.0/24).

In a peer-to-peer configuration, you need to define a policy address for the private IP address of a server or host behind the remote VPN peer (for example, 172.16.5.1/255.255.255.255, 172.16.5.1/32, or 172.16.5.1).

For a FortiGate dialup server in a dialup-client or internet-browsing configuration, the source IP should reflect the IP addresses of the dialup clients:

## Defining security policies

Policy-based and route-based VPNs require different security policies.

- A policy-based VPN requires an IPsec policy. You specify the interface to the private network, the interface to the remote peer and the VPN tunnel. A single policy can enable traffic inbound, outbound, or in both directions.
- A route-based VPN requires an accept policy for each direction. For the source and destination interfaces, you specify the interface to the private network and the virtual IPsec interface (phase 1 configuration) of the VPN. The IPsec interface is the destination interface for the outbound policy and the source interface for the inbound policy. One security policy must be configured for each direction of each VPN interface.



If the policy that grants the VPN connection is limited to certain services, DHCP must be included, otherwise the client will not be able to retrieve a lease from the FortiGate's (IPsec) DHCP server because the DHCP request (coming out of the tunnel) will be blocked.

---

## Policy-based VPN

An IPsec policy enables the transmission and reception of encrypted packets, specifies the permitted direction of VPN traffic, and selects the VPN tunnel. In most cases, a single policy is needed to control both inbound and outbound IP traffic through a VPN tunnel. For a detailed example, see [Policy-based IPsec tunnel on page 1164](#). Be aware of the following before creating an IPsec policy.

## Allow traffic to be initiated from the remote site

Policies specify which IP addresses can initiate a tunnel. By default, traffic from the local private network initiates the tunnel. When the *Allow traffic to be initiated from the remote site* option is selected, traffic from a dialup client, or a computer on a remote network, initiates the tunnel. Both can be enabled at the same time for bi-directional initiation of the tunnel.

## Outbound and inbound NAT

When a FortiGate operates in NAT mode, you can enable inbound or outbound NAT. Outbound NAT may be performed on outbound encrypted packets or IP packets in order to change their source address before they are sent through the tunnel. Inbound NAT is performed to intercept and decrypt emerging IP packets from the tunnel.

By default, these options are not selected in security policies and can only be set through the CLI.

## Defining multiple IPsec policies for the same tunnel

You must define at least one IPsec policy for each VPN tunnel. If the same remote server or client requires access to more than one network behind a local FortiGate, the FortiGate must be configured with an IPsec policy for each network. Multiple policies may be required to configure redundant connections to a remote destination or control access to different services at different times.

To ensure a secure connection, the FortiGate must evaluate policies with *Action* set to *IPsec* before *ACCEPT* and *DENY*. Because the FortiGate unit reads policies starting at the top of the list, you must move all IPsec policies to the top of the list, and be sure to reorder your multiple IPsec policies that apply to the tunnel so that specific constraints can be evaluated before general constraints. If you create two equivalent IPsec policies for two different tunnels, the system will select the correct policy based on the specified source and destination addresses.



Adding multiple IPsec policies for the same VPN tunnel can cause conflicts if the policies specify similar source and destination addresses, but have different settings for the same service. When policies overlap in this manner, the system may apply the wrong IPsec policy or the tunnel may fail.

### Route-based VPN

When you define a route-based VPN, you create a virtual IPsec interface on the physical interface that connects to the remote peer. You create ordinary accept policies to enable traffic between the IPsec interface and the interface that connects to the private network. This makes configuration simpler than for policy-based VPNs.

#### To configure policies for a route-based VPN:

1. Go to *Policy & Objects > Firewall Policy*.
2. Click *Create New* and define an *ACCEPT* policy to permit communication between the local private network and the private network behind the remote peer and enter these settings in particular:

<b>Name</b>	Enter a name for the security policy.
<b>Incoming Interface</b>	Select the interface that connects to the private network behind this FortiGate.
<b>Outgoing Interface</b>	Select the IPsec interface you configured.
<b>Source</b>	Select the address name you defined for the private network behind this FortiGate.
<b>Destination</b>	Select the address name you defined for the private network behind the remote peer.
<b>Action</b>	Select <i>ACCEPT</i> .
<b>NAT</b>	Disable <i>NAT</i> .

3. Click *OK*.  
To permit the remote client to initiate communication, you need to define a security policy for communication in that direction.

- Click *Create New* and enter these settings in particular:

<b>Name</b>	Enter a name for the security policy.
<b>Incoming Interface</b>	Select the IPsec interface you configured.
<b>Outgoing Interface</b>	Select the interface that connects to the private network behind this FortiGate.
<b>Source</b>	Select the address name you defined for the private network behind the remote peer.
<b>Destination</b>	Select the address name you defined for the private network behind this FortiGate.
<b>Action</b>	Select <i>ACCEPT</i> .
<b>NAT</b>	Disable <i>NAT</i> .

- Click *OK*.

## Blocking unwanted IKE negotiations and ESP packets with a local-in policy

It is not unusual to receive IPsec connection attempts or malicious IKE packets from all over the internet. Malicious parties use these probes to try to establish an IPsec tunnel in order to gain access to your private network. A good way to prevent this is to use local-in policies to deny such traffic.

Sometimes there are malicious attempts using crafted invalid ESP packets. These invalid attempts are automatically blocked by the FOS IPsec local-in handler when it checks the SPI value against the SAs of existing tunnels. The IPsec local-in handler processes the packet instead of the firewall's local-in handler. So when these attempts are blocked, you will notice an `unknown SPI` message in your VPN logs instead of being silently blocked by your local-in policy. These log messages are rate limited.

### Sample log and alert email

Message meets Alert condition

```
date=2020-08-11 time=09:28:40 devname=toSite1 devid=FGT60Fxxxxxxxxx logid="0101037131"
type="event" subtype="vpn" level="error" vd="root" eventtime=1597163320747963100 tz="-0700"
logdesc="IPsec ESP" msg="IPsec ESP" action="error" remip=131.62.25.102 locip=192.157.116.88
remport=40601 locport=500 outintf="wan1" cookies="N/A" user="N/A" group="N/A"
xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="N/A" status="esp_error" error_
num="Received ESP packet with unknown SPI." spi="f6c9e2x1" seq="02000400"
```

Note that invalid SPIs may not always indicate malicious activity. For example, the SPI may not match during rekey, or when one unit flushes its tunnel SAs. Administrators should collect as much information as possible before making a conclusion.

### To block undesirable IPsec connection attempts and IKE packets using a local-in policy:

- Configure an address group that excludes legitimate IPs:

```
config firewall addrgrp
 edit "All_exceptions"
 set member "all"
 set exclude enable
 set exclude-member "remote-vpn"
```



```

 next
end

```

## 2. Create a local-in policy that blocks IKE traffic from the address group:

```

config firewall local-in-policy
 edit 1
 set intf "wan1"
 set srcaddr "All_exceptions"
 set dstaddr "all"
 set service "IKE"
 set schedule "always"
 next
end

```



The default action is deny.

## 3. Verify the traffic blocked by the local-in policy:

```

diagnose debug flow filter dport 500
diagnose debug flow trace start 10
diagnose debug enable

id=20085 trace_id=290 func=print_pkt_detail line=5588 msg="vd-root:0 received a packet
(proto=17, 10.10.10.13:500->10.10.10.1:500) from wan1. "
id=20085 trace_id=290 func=init_ip_session_common line=5760 msg="allocate a new session-
003442e7"
id=20085 trace_id=290 func=vf_ip_route_input_common line=2598 msg="find a route:
flag=84000000 gw-10.10.10.1 via root"
id=20085 trace_id=290 func=fw_local_in_handler line=430 msg="iprope_in_check() check
failed on policy 1, drop"

```

## Site-to-site VPN

A site-to-site VPN connection lets branch offices use the Internet to access the main office's intranet. A site-to-site VPN allows offices in multiple, fixed locations to establish secure connections with each other over a public network such as the Internet.

The following sections provide instructions for configuring site-to-site VPNs:

- [FortiGate-to-FortiGate on page 1139](#)
- [FortiGate-to-third-party on page 1171](#)

### FortiGate-to-FortiGate

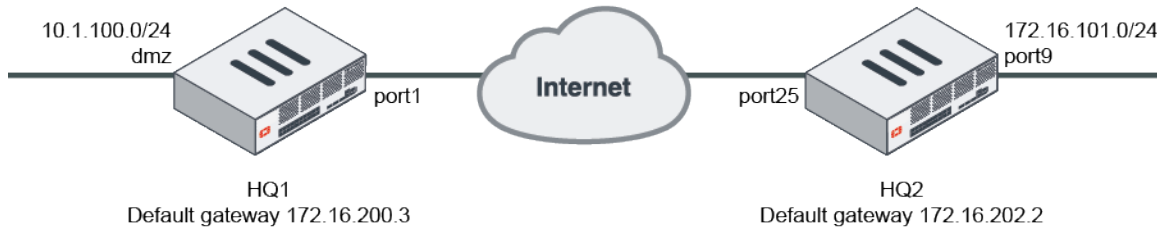
This section contains the following topics about FortiGate-to-FortiGate VPN configurations:

- [Basic site-to-site VPN with pre-shared key on page 1140](#)
- [Site-to-site VPN with digital certificate on page 1145](#)
- [Site-to-site VPN with overlapping subnets on page 1151](#)

- [GRE over IPsec on page 1160](#)
- [Policy-based IPsec tunnel on page 1164](#)

## Basic site-to-site VPN with pre-shared key

This is a sample configuration of IPsec VPN authenticating a remote FortiGate peer with a pre-shared key.



### To configure IPsec VPN authenticating a remote FortiGate peer with a pre-shared key in the GUI:

1. Configure the HQ1 FortiGate.
  - a. Go to **VPN > IPsec Wizard** and configure the following settings for **VPN Setup**:
    - i. Enter a VPN name.
    - ii. For *Template Type*, select *Site to Site*.
    - iii. For *Remote Device Type*, select *FortiGate*.
    - iv. For *NAT Configuration*, select *No NAT Between Sites*.
    - v. Click *Next*.
  - b. Configure the following settings for *Authentication*:
    - i. For *Remote Device*, select *IP Address*.
    - ii. For the IP address, enter *172.16.202.1*.
    - iii. For *Outgoing interface*, enter *port1*.
    - iv. For *Authentication Method*, select *Pre-shared Key*.
    - v. In the *Pre-shared Key* field, enter *sample* as the key.
    - vi. Click *Next*.
  - c. Configure the following settings for *Policy & Routing*:
    - i. From the *Local Interface* dropdown menu, select the local interface.
    - ii. Configure the *Local Subnets* as *10.1.100.0*.
    - iii. Configure the *Remote Subnets* as *172.16.101.0*.
    - iv. Click *Create*.
2. Configure the HQ2 FortiGate.
  - a. Go to **VPN > IPsec Wizard** and configure the following settings for **VPN Setup**:
    - i. Enter a VPN name.
    - ii. For *Template Type*, select *Site to Site*.
    - iii. For *Remote Device Type*, select *FortiGate*.
    - iv. For *NAT Configuration*, select *No NAT Between Sites*.
    - v. Click *Next*.
  - b. Configure the following settings for *Authentication*:
    - i. For *Remote Device*, select *IP Address*.
    - ii. For the IP address, enter *172.16.200.1*.
    - iii. For *Outgoing interface*, enter *port25*.

- iv. For *Authentication Method*, select *Pre-shared Key*.
- v. In the *Pre-shared Key* field, enter *sample* as the key.
- vi. Click *Next*.
- c. Configure the following settings for *Policy & Routing*:
  - i. From the *Local Interface* dropdown menu, select the local interface.
  - ii. Configure *Local Subnets* as *172.16.101.0*.
  - iii. Configure the *Remote Subnets* as *10.1.100.0*.
  - iv. Click *Create*.

### To configure IPsec VPN authenticating a remote FortiGate peer with a pre-shared key using the CLI:

1. Configure the WAN interface and default route. The WAN interface is the interface connected to the ISP. The IPsec tunnel is established over the WAN interface.

- a. Configure HQ1.

```
config system interface
 edit "port1"
 set vdom "root"
 set ip 172.16.200.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 172.16.200.3
 set device "port1"
 next
end
```

- b. Configure HQ2.

```
config system interface
 edit "port25"
 set vdom "root"
 set ip 172.16.202.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 172.16.202.2
 set device "port25"
 next
end
```

2. Configure the internal (protected subnet) interface. The internal interface connects to the corporate internal network. Traffic from this interface routes out the IPsec VPN tunnel.

- a. Configure HQ1.

```
config system interface
 edit "dmz"
 set vdom "root"
 set ip 10.1.100.1 255.255.255.0
 next
end
```

**b. Configure HQ2.**

```
config system interface
 edit "port9"
 set vdom "root"
 set ip 172.16.101.1 255.255.255.0
 next
end
```

**3. Configure the IPsec phase1-interface.****a. Configure HQ1.**

```
config vpn ipsec phase1-interface
 edit "to_HQ2"
 set interface "port1"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.16.202.1
 set psksecret sample
 next
end
```

**b. Configure HQ2.**

```
config vpn ipsec phase1-interface
 edit "to_HQ1"
 set interface "port25"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.16.200.1
 set psksecret sample
 next
end
```

**4. Configure the IPsec phase2-interface.****a. Configure HQ1.**

```
config vpn ipsec phase2-interface
 edit "to_HQ2"
 set phase1name "to_HQ2"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 set auto-negotiate enable
 next
end
```

**b. Configure HQ2.**

```
config vpn ipsec phase2-interface
 edit "to_HQ2"
 set phase1name "to_HQ1"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 set auto-negotiate enable
 next
end
```

5. Configure the static routes. Two static routes are added to reach the remote protected subnet. The blackhole route is important to ensure that IPsec traffic does not match the default route when the IPsec tunnel is down.

a. Configure HQ1.

```
config router static
 edit 2
 set dst 172.16.101.0 255.255.255.0
 set device "to_HQ2"
 next
 edit 3
 set dst 172.16.101.0 255.255.255.0
 set blackhole enable
 set distance 254
 next
end
```

b. Configure HQ2.

```
config router static
 edit 2
 set dst 10.1.100.0 255.255.255.0
 set device "to_HQ1"
 next
 edit 3
 set dst 10.1.100.0 255.255.255.0
 set blackhole enable
 set distance 254
 next
end
```

6. Configure two firewall policies to allow bidirectional IPsec traffic flow over the IPsec VPN tunnel.

a. Configure HQ1.

```
config firewall policy
 edit 1
 set name "inbound"
 set srcintf "to_HQ2"
 set dstintf "dmz"
 set srcaddr "172.16.101.0"
 set dstaddr "10.1.100.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set name "outbound"
 set srcintf "dmz"
 set dstintf "to_HQ2"
 set srcaddr "10.1.100.0"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end
```

**b. Configure HQ2.**

```

config firewall policy
 edit 1
 set name "inbound"
 set srcintf "to_HQ1"
 set dstintf "port9"
 set srcaddr "10.1.100.0"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set name "outbound"
 set srcintf "port9"
 set dstintf "to_HQ1"
 set srcaddr "172.16.101.0"
 set dstaddr "10.1.100.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end

```

- 7. Run diagnose commands.** The `diagnose debug application ike -1` command is the key to troubleshoot why the IPsec tunnel failed to establish. If the PSK failed to match, the following error shows up in the debug output:

```

ike 0:to_HQ2:15037: parse error
ike 0:to_HQ2:15037: probable pre-shared secret mismatch'

```

The following commands are useful to check IPsec phase1/phase2 interface status.

- a. Run the `diagnose vpn ike gateway list` command on HQ1.** The system should return the following:

```

vd: root/0
name: to_HQ2
version: 1
interface: port1 11
addr: 172.16.200.1:500 -> 172.16.202.1:500
created: 5s ago
IKE SA: created 1/1 established 1/1 time 0/0/0 ms
IPsec SA: created 2/2 established 2/2 time 0/0/0 ms
id/spi: 12 6e8d0532e7fe8d84/3694ac323138a024
direction: responder
status: established 5-5s ago = 0ms
proposal: aes128-sha256
key: b3efb46d0d385aff-7bb9ee241362ee8d
lifetime/rekey: 86400/86124
DPD sent/recvd: 00000000/00000000

```

- b. Run the `diagnose vpn tunnel list` command on HQ1.** The system should return the following:

```

list all ipsec tunnel in vd 0
name=to_HQ2 ver=1 serial=1 172.16.200.1:0->172.16.202.1:0
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_
dev frag-rfcaccept_traffic=1
proxyid_num=1 child_num=0 refcnt=11 ilast=7 olast=87 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0

```

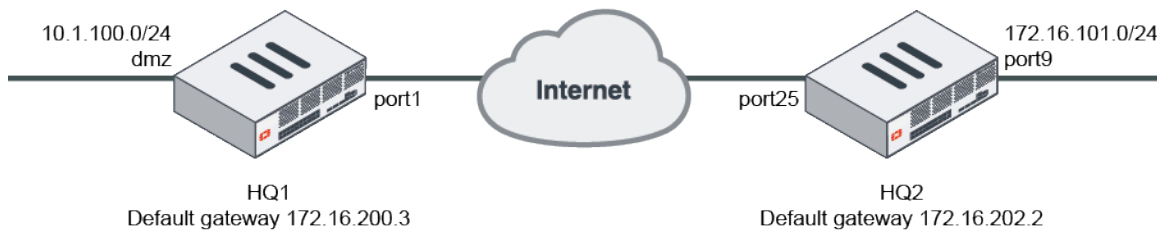
```

dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=to_HQ2 proto=0 sa=1 ref=2 serial=1 auto-negotiate
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=3 options=18227 type=00 soft=0 mtu=1438 expire=42927/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000000 itn=0
life: type=01 bytes=0/0 timeout=42930/43200
dec: spi=ef9ca700 esp=aes key=16 a2c6584bf654d4f956497b3436f1cfc7
ah=sha1 key=20 82c5e734bce81e6f18418328e2a11aeb7baa021b
enc: spi=791e898e esp=aes key=16 0dbb4588ba2665c6962491e85a4a8d5a
ah=sha1 key=20 2054b318d2568a8b12119120f20ecac97ab730b3
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0

```

## Site-to-site VPN with digital certificate

This is a sample configuration of IPsec VPN authenticating a remote FortiGate peer with a certificate. The certificate on one peer is validated by the presence of the CA certificate installed on the other peer.



### To configure IPsec VPN authenticating a remote FortiGate peer with a digital certificate in the GUI:

1. Import the certificate.
2. Configure user peers.
3. Configure the HQ1 FortiGate.
  - a. Go to **VPN > IPsec Wizard** and configure the following settings for *VPN Setup*:
    - i. Enter a VPN name.
    - ii. For *Template Type*, select *Site to Site*.
    - iii. For *Remote Device Type*, select *FortiGate*.
    - iv. For *NAT Configuration*, select *No NAT Between Sites*.
    - v. Click *Next*.
  - b. Configure the following settings for *Authentication*:
    - i. For *Remote Device*, select *IP Address*.
    - ii. For the IP address, enter *172.16.202.1*.
    - iii. For *Outgoing interface*, enter *port1*.
    - iv. For *Authentication Method*, select *Signature*.
    - v. In the *Certificate name* field, select the imported certificate.
    - vi. From the *Peer Certificate CA* dropdown list, select the desired peer CA certificate.
    - vii. Click *Next*.
  - c. Configure the following settings for *Policy & Routing*:
    - i. From the *Local Interface* dropdown menu, select the local interface.
    - ii. Configure the *Local Subnets* as *10.1.100.0*.

- iii. Configure the *Remote Subnets* as *172.16.101.0*.
  - iv. Click *Create*.
- 4. Configure the HQ2 FortiGate.
  - a. Go to *VPN > IPsec Wizard* and configure the following settings for *VPN Setup*:
    - i. Enter a VPN name.
    - ii. For *Template Type*, select *Site to Site*.
    - iii. For *Remote Device Type*, select *FortiGate*.
    - iv. For *NAT Configuration*, select *No NAT Between Sites*.
    - v. Click *Next*.
  - b. Configure the following settings for *Authentication*:
    - i. For *Remote Device*, select *IP Address*.
    - ii. For the IP address, enter *172.16.200.1*.
    - iii. For *Outgoing interface*, enter *port25*.
    - iv. For *Authentication Method*, select *Signature*.
    - v. In the *Certificate name* field, select the imported certificate.
    - vi. From the *Peer Certificate CA* dropdown list, select the peer CA certificate.
    - vii. Click *Next*.
  - c. Configure the following settings for *Policy & Routing*:
    - i. From the *Local Interface* dropdown menu, select the local interface.
    - ii. Configure *Local Subnets* as *172.16.101.0*.
    - iii. Configure the *Remote Subnets* as *10.1.100.0*.
    - iv. Click *Create*.

### To configure IPsec VPN authenticating a remote FortiGate peer with a digital certificate using the CLI:

1. Configure the WAN interface and default route. The WAN interface is the interface connected to the ISP. The IPsec tunnel is established over the WAN interface.

- a. Configure HQ1.

```
config system interface
 edit "port1"
 set vdom "root"
 set ip 172.16.200.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 172.16.200.3
 set device "port1"
 next
end
```

- b. Configure HQ2.

```
config system interface
 edit "port25"
 set vdom "root"
 set ip 172.16.202.1 255.255.255.0
 next
end
config router static
```



```
edit 1
 set gateway 172.16.202.2
 set device "port25"
next
end
```

- 2. Configure the internal (protected subnet) interface. The internal interface connects to the corporate internal network. Traffic from this interface routes out the IPsec VPN tunnel.**

**a. Configure HQ1.**

```
config system interface
 edit "dmz"
 set vdom "root"
 set ip 10.1.100.1 255.255.255.0
 next
end
```

**b. Configure HQ2.**

```
config system interface
 edit "port9"
 set vdom "root"
 set ip 172.16.101.1 255.255.255.0
 next
end
```

- 3. Configure the import certificate and its CA certificate information. The certificate and its CA certificate must be imported on the remote peer FortiGate and on the primary FortiGate before configuring IPsec VPN tunnels. If the built-in Fortinet\_Factory certificate and the Fortinet\_CA CA certificate are used for authentication, you can skip this step.**

**a. Configure HQ1.**

```
config vpn certificate local
 edit "test1"
 ...
 set range global
 next
end
config vpn certificate ca
 edit "CA_Cert_1"
 ...
 set range global
 next
end
```

**b. Configure HQ2.**

```
config vpn certificate local
 edit "test2"
 ...
 set range global
 next
end
config vpn certificate ca
 edit "CA_Cert_1"
 ...
 set range global
```

```

 next
end

```

4. Configure the peer user. The peer user is used in the IPsec VPN tunnel peer setting to authenticate the remote peer FortiGate.

- a. If not using the built-in Fortinet\_Factory certificate and Fortinet\_CA CA certificate, do the following:

- i. Configure HQ1.

```

config user peer
 edit "peer1"
 set ca "CA_Cert_1"
 next
end

```

- ii. Configure HQ2.

```

config user peer
 edit "peer2"
 set ca "CA_Cert_1"
 next
end

```

- b. If the built-in Fortinet\_Factory certificate and Fortinet\_CA CA certificate are used for authentication, the peer user must be configured based on Fortinet\_CA.

- i. Configure HQ1.

```

config user peer
 edit "peer1"
 set ca "Fortinet_CA"
 next
end

```

- ii. Configure HQ2.

```

config user peer
 edit "peer2"
 set ca "Fortinet_CA"
 next
end

```

5. Configure the IPsec phase1-interface.

- a. Configure HQ1.

```

config vpn ipsec phase1-interface
 edit "to_HQ2"
 set interface "port1"
 set authmethod signature
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.16.202.1
 set certificate "test1"
 set peer "peer1"
 next
end

```

- b. Configure HQ2.

```

config vpn ipsec phase1-interface
 edit "to_HQ1"

```

```
 set interface "port25"
 set authmethod signature
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.16.200.1
 set certificate "test2"
 set peer "peer2"
 next
end
```

## 6. Configure the IPsec phase2-interface.

### a. Configure HQ1.

```
config vpn ipsec phase2-interface
 edit "to_HQ2"
 set phase1name "to_HQ2"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 set auto-negotiate enable
 next
end
```

### b. Configure HQ2.

```
config vpn ipsec phase2-interface
 edit "to_HQ2"
 set phase1name "to_HQ1"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 set auto-negotiate enable
 next
end
```

## 7. Configure the static routes. Two static routes are added to reach the remote protected subnet. The blackhole route is important to ensure that IPsec traffic does not match the default route when the IPsec tunnel is down.

### a. Configure HQ1.

```
config router static
 edit 2
 set dst 172.16.101.0 255.255.255.0
 set device "to_HQ2"
 next
 edit 3
 set dst 172.16.101.0 255.255.255.0
 set blackhole enable
 set distance 254
 next
end
```

### b. Configure HQ2.

```
config router static
 edit 2
 set dst 10.1.100.0 255.255.255.0
 set device "to_HQ1"
 next
 edit 3
 set dst 10.1.100.0 255.255.255.0
```

```

 set blackhole enable
 set distance 254
 next
end

```

**8. Configure two firewall policies to allow bidirectional IPsec traffic flow over the IPsec VPN tunnel.**

**a. Configure HQ1.**

```

config firewall policy
 edit 1
 set name "inbound"
 set srcintf "to_HQ2"
 set dstintf "dmz"
 set srcaddr "172.16.101.0"
 set dstaddr "10.1.100.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set name "outbound"
 set srcintf "dmz"
 set dstintf "to_HQ2"
 set srcaddr "10.1.100.0"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end

```

**b. Configure HQ2.**

```

config firewall policy
 edit 1
 set name "inbound"
 set srcintf "to_HQ1"
 set dstintf "port9"
 set srcaddr "10.1.100.0"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set name "outbound"
 set srcintf "port9"
 set dstintf "to_HQ1"
 set srcaddr "172.16.101.0"
 set dstaddr "10.1.100.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end

```

**9. Run diagnose commands.** The diagnose debug application ike -l command is the key to troubleshoot why the IPsec tunnel failed to establish. If the remote FortiGate certificate cannot be validated, the following error

shows up in the debug output:

```
ike 0: to_HQ2:15314: certificate validation failed
```

The following commands are useful to check IPsec phase1/phase2 interface status.

- a. Run the `diagnose vpn ike gateway list` command on HQ1. The system should return the following:

```
vd: root/0
name: to_HQ2
version: 1
interface: port1 11
addr: 172.16.200.1:500 -> 172.16.202.1:500
created: 7s ago
peer-id: C = CA, ST = BC, L = Burnaby, O = Fortinet, OU = QA, CN = test2
peer-id-auth: yes
IKE SA: created 1/1 established 1/1 time 70/70/70 ms
IPsec SA: created 1/1 established 1/1 time 80/80/80 ms
id/spi: 15326 295be407fbddfc13/7a5a52afa56adf14 direction: initiator status:
established 7-7s ago = 70ms proposal: aes128-sha256 key: 4aa06dbec359a4c7-
43570710864bcf7b lifetime/rekey: 86400/86092 DPD sent/recvd: 00000000/00000000 peer-
id: C = CA, ST = BC, L = Burnaby, O = Fortinet, OU = QA, CN = test2
```

- b. Run the `diagnose vpn tunnel list` command on HQ1. The system should return the following:

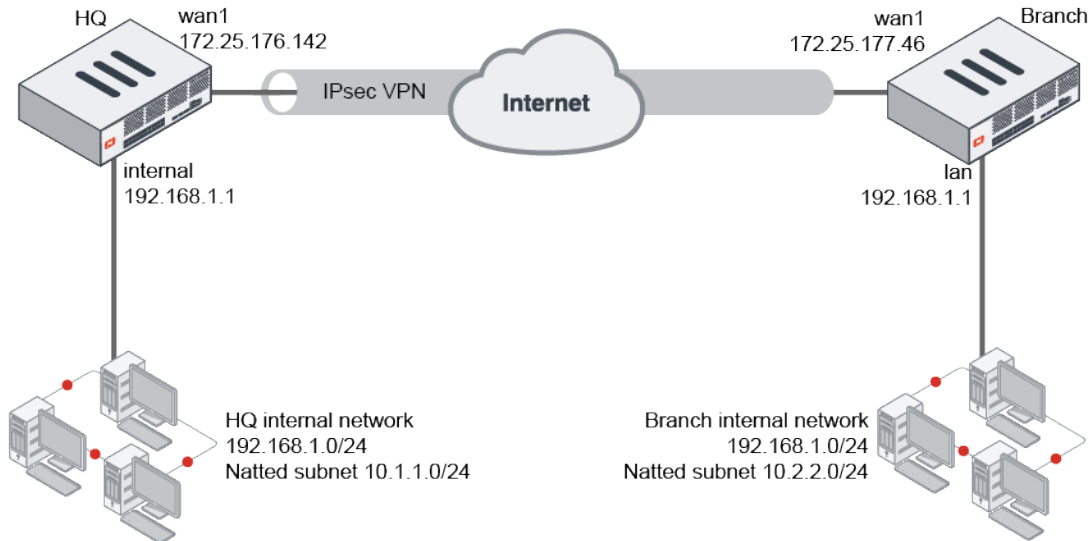
```
list all ipsec tunnel in vd 0
name=to_HQ2 ver=1 serial=1 172.16.200.1:0->172.16.202.1:0
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_
dev frag-rfcaccept_traffic=1
proxyid_num=1 child_num=0 refcnt=14 ilast=19 olast=179 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=vpn-f proto=0 sa=1 ref=2 serial=1 auto-negotiate
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=3 options=18227 type=00 soft=0 mtu=1438 expire=42717/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000000 itn=0
life: type=01 bytes=0/0 timeout=42897/43200
dec: spi=72e87de7 esp=aes key=16 8b2b93e0c149d6f22b1c0b96ea450e6c
ah=sha1 key=20 facc655e5f33beb7c2b12e718a6d55413ce3efa2
enc: spi=5c52c865 esp=aes key=16 8d0c4e4adbf2338beed569b2b3205ece
ah=sha1 key=20 553331628612480ab6d7d563a00e2a967ebabccdd
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

## Site-to-site VPN with overlapping subnets

This is a sample configuration of IPsec VPN to allow transparent communication between two overlapping networks that are located behind different FortiGates using a route-based tunnel with source and destination NAT.

In the following topology, both FortiGates (HQ and Branch) use 192.168.1.0/24 as their internal network, but both networks need to be able to communicate to each other through the IPsec tunnel.

New virtual subnets of equal size must be configured and used for all communication between the two overlapping subnets. The devices on both local networks do not need to change their IP addresses. However, the devices and users must use the new subnet range of the remote network to communicate across the tunnel.



## Configuring the HQ FortiGate

### To configure IPsec VPN:

1. Go to **VPN > IPsec Wizard** and select the *Custom* template.
2. Enter the name *VPN-to-Branch* and click *Next*.
3. For the *IP Address*, enter the Branch public IP address (*172.25.177.46*), and for *Interface*, select the HQ WAN interface (*wan1*).

Network	
IP Version	<span style="background-color: #28a745; color: white;">IPv4</span> IPv6
Remote Gateway	Static IP Address
IP Address	172.25.177.46
Interface	wan1

4. For *Pre-shared Key*, enter a secure key. You will use the same key when configuring IPsec VPN on the Branch FortiGate.

Authentication	
Method	Pre-shared Key
Pre-shared Key	.....

5. In the *Phase 2 Selectors* section, enter the subnets for the *Local Address* (*10.1.1.0/24*) and *Remote Address* (*10.2.2.0/24*).

Phase 2 Selectors		
Name	Local Address	Remote Address
VPN-to-Branch	10.1.1.0/24	10.2.2.0/24
<div>New Phase 2 <span style="float: right;">+ - ↺</span></div> <div> <div>Name</div> <div>VPN-to-Branch</div> </div> <div> <div>Comments</div> <div>Comments</div> </div> <div> <div>Local Address</div> <div>Subnet 10.1.1.0/24</div> </div> <div> <div>Remote Address</div> <div>Subnet 10.2.2.0/24</div> </div> <div> <div>Advanced...</div> </div>		

6. Optionally, expand *Advanced* and enable *Auto-negotiate*.

Auto-negotiate	<input checked="" type="checkbox"/>
Autokey Keep Alive	<input checked="" type="checkbox"/>

- Click **OK**.

### To configure the static routes:

- Go to **Network > Static Routes** and click **Create New**.
- In the **Destination** field, enter the remote address subnet (**10.2.2.0/24**).
- For **Interface**, select the VPN tunnel you just created, **VPN-to-Branch**.

Destination	<b>Subnet</b>   Named Address   Internet Service
	10.2.2.0/24
Interface	VPN-to-Branch
Administrative Distance	10

- Click **OK**.
- Create another route with the same **Destination**, but change the **Administrative Distance** to **200** and for **Interface**, select **Blackhole**. This is a best practice for route-based IPsec VPN tunnels because it ensures traffic for the remote FortiGate's subnet is not sent using the default route in the event that the IPsec tunnel goes down.

Destination	<b>Subnet</b>   Named Address   Internet Service
	10.2.2.0/24
Interface	Blackhole
Administrative Distance	200

### To configure the address objects:

- Go to **Policy & Objects > Addresses** and click **Create New > Address**.
- For **Name**, enter **HQ-original**.
- For **IP/Netmask**, enter the original LAN subnet of HQ (**192.168.1.0/24**).
- For **Interface**, select the LAN-side interface (**internal**).

Name	HQ-original
Color	Change
Type	Subnet
IP/Netmask	192.168.1.0/24
Interface	internal

- Click **OK**.
- Create another address object named **Branch-new**, but for **IP/Netmask**, enter the new LAN subnet of Branch (**10.2.2.0/24**), and select the VPN interface (**VPN-to-Branch**).

Name	Branch-new
Color	Change
Type	Subnet
IP/Netmask	10.2.2.0/24
Interface	VPN-to-Branch

### To configure the IP pool:

- Go to **Policy & Objects > IP Pools** and click **Create New**.
- For **Name**, enter **HQ-new**.
- For **Type**, select **Fixed Port Range**.
- Enter the **External IP address/range** (**10.1.1.1 – 10.1.1.254**, the new HQ subnet) and **Internal IP Range** (**192.168.1.1 – 192.168.1.254**, the original HQ subnet).

Name	HQ-new
Comments	
Type	Overload One-to-One <b>Fixed Port Range</b> Port Block Allocation
External IP address/range ⓘ	10.1.1.1-10.1.1.254
Internal IP Range ⓘ	192.168.1.1-192.168.1.254
ARP Reply	<input checked="" type="checkbox"/>

5. Click **OK**.

### To configure the VIP:

1. Go to *Policy & Objects* > *Virtual IPs* and click *Create New* > *Virtual IP*.
2. For *Name*, enter *HQ-new-to-original*.
3. For *Interface*, select the VPN interface (*VPN-to-Branch*).
4. Enter the *External IP address/range* (10.1.1.1 – 10.1.1.254, the new HQ subnet) and *Mapped IP address/range* (192.168.1.1 – 192.168.1.254, the original HQ subnet).

Name	HQ-new-to-original
Comments	<input type="text"/> 0/255
Color	<input type="button" value="Change"/>

Network	
Interface	VPN-to-Branch
Type	Static NAT
External IP address/range	10.1.1.1-10.1.1.254
Mapped IP address/range	192.168.1.1-192.168.1.254

5. Click **OK**.

### To configure the firewall policy for traffic from HQ to Branch:

1. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*.
2. For *Name*, enter *From-HQ-to-Branch*.
3. For *Incoming Interface*, select the LAN-side interface (*internal*).
4. For *Outgoing Interface*, select the VPN tunnel interface (*VPN-to-Branch*).
5. For *Source*, select *HQ-original*.
6. For *Destination*, select *Branch-new*.
7. For *Service*, select *ALL*.
8. Enable *NAT*.



9. Select *Use Dynamic IP Pool* and select the *HQ-new* IP pool.

Name	From-HQ-to-Branch
Incoming Interface	internal
Outgoing Interface	VPN-to-Branch
Source	HQ-original
Destination	Branch-new
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based
Firewall / Network Options	
NAT	<input checked="" type="checkbox"/>
IP Pool Configuration	<input type="checkbox"/> Use Outgoing Interface Address <input checked="" type="checkbox"/> Use Dynamic IP Pool
	HQ-new

10. Click OK.

### To configure the firewall policy for traffic from Branch to HQ:

1. Click *Create New* and for *Name*, enter *From-Branch-to-HQ*.
2. For *Incoming Interface*, select the VPN tunnel interface (*VPN-to-Branch*).
3. For *Outgoing Interface*, select the LAN-side interface (*internal*).
4. For *Source*, select *Branch-new*.
5. For *Destination*, select the *HQ-new-to-original* VIP.
6. For *Service*, select *ALL*.
7. Disable NAT.

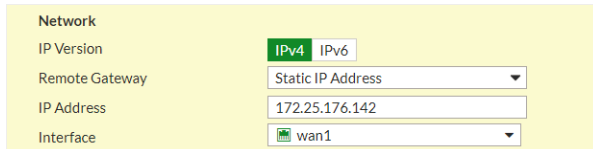
Name	From-Branch-to-HQ
Incoming Interface	VPN-to-Branch
Outgoing Interface	internal
Source	Branch-new
Destination	HQ-new-to-original
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based
Firewall / Network Options	
NAT	<input type="checkbox"/>

8. Click OK.

## Configuring the Branch FortiGate

### To configure IPsec VPN:

1. Go to *VPN > IPsec Wizard* and select the *Custom* template.
2. Enter the name *VPN-to-HQ* and click *Next*.
3. For the *IP Address*, enter the HQ public IP address (*172.25.176.142*), and for *Interface*, select the Branch WAN interface (*wan1*).



Network

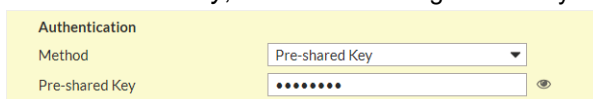
IP Version: IPv4 | IPv6

Remote Gateway: Static IP Address

IP Address: 172.25.176.142

Interface: wan1

4. For *Pre-shared Key*, enter the matching secure key used in the *VPN-to-Branch* tunnel.

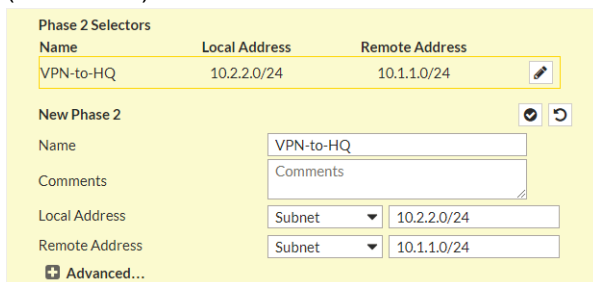


Authentication

Method: Pre-shared Key

Pre-shared Key: .....

5. In the *Phase 2 Selectors* section, enter the subnets for the *Local Address* (*10.2.2.0/24*) and *Remote Address* (*10.1.1.0/24*).



Phase 2 Selectors

Name	Local Address	Remote Address
VPN-to-HQ	10.2.2.0/24	10.1.1.0/24

New Phase 2

Name: VPN-to-HQ

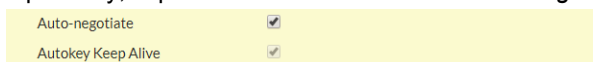
Comments:

Local Address: Subnet 10.2.2.0/24

Remote Address: Subnet 10.1.1.0/24

Advanced...

6. Optionally, expand *Advanced* and enable *Auto-negotiate*.



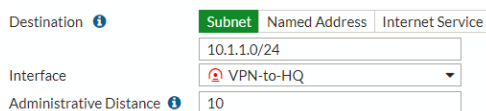
Auto-negotiate: ☒

Autokey Keep Alive: ☒

7. Click *OK*.

### To configure the static routes:

1. Go to *Network > Static Routes* and click *Create New*.
2. In the *Destination* field, enter the remote address subnet (*10.1.1.0/24*).
3. For *Interface*, select the VPN tunnel you just created, *VPN-to-HQ*.



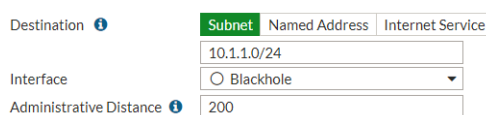
Destination: Subnet | Named Address | Internet Service

10.1.1.0/24

Interface: VPN-to-HQ

Administrative Distance: 10

4. Click *OK*.
5. Create another route with the same *Destination*, but change the *Administrative Distance* to *200* and for *Interface*, select *Blackhole*.



Destination: Subnet | Named Address | Internet Service

10.1.1.0/24

Interface: Blackhole

Administrative Distance: 200

### To configure the address objects:

1. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
2. For *Name*, enter *Branch-original*.
3. For *IP/Netmask*, enter the original LAN subnet of Branch (*192.168.1.0/24*).
4. For *Interface*, select the LAN-side interface (*lan*).

Name	Branch-original
Color	Change
Type	Subnet
Subnet / IP Range	192.168.1.0/24
Interface	lan

5. Click *OK*
6. Create another address object named *HQ-new*, but for *IP/Netmask*, enter the new LAN subnet of HQ (*10.1.1.0/24*), and select the VPN interface (*VPN-to-HQ*).

Name	HQ-new
Color	Change
Type	Subnet
Subnet / IP Range	10.1.1.0/24
Interface	VPN-to-HQ

### To configure the IP pool:

1. Go to *Policy & Objects > IP Pools* and click *Create New*.
2. For *Name*, enter *Branch-new*.
3. For *Type*, select *Fixed Port Range*.
4. Enter the *External IP address/range* (*10.2.2.1 – 10.2.2.254*, the new Branch subnet) and *Internal IP Range* (*192.168.1.1 – 192.168.1.254*, the original Branch subnet).

Name	Branch-new
Comments	
Type	Overload One-to-One <b>Fixed Port Range</b> Port Block Allocation
External IP address/range ⓘ	10.2.2.1-10.2.2.254
Internal IP Range ⓘ	192.168.1.1-192.168.1.254
ARP Reply	

5. Click *OK*.

### To configure the VIP:

1. Go to *Policy & Objects > Virtual IPs* and click *Create New > Virtual IP*.
2. For *Name*, enter *Branch-new-to-original*.
3. For *Interface*, select the VPN interface (*VPN-to-HQ*).
4. Enter the *External IP address/range* (*10.2.2.1 – 10.2.2.254*, the new Branch subnet) and *Mapped IP address/range* (*192.168.1.1 – 192.168.1.254*, the original Branch subnet).

Name	Branch-new-to-original
Comments	
Color	Change
Network	
Interface	VPN-to-HQ
Type	Static NAT
External IP address/range	10.2.2.1-10.2.2.254
Mapped IP address/range	192.168.1.1-192.168.1.254

5. Click **OK**.

### To configure the firewall policy for traffic from Branch to HQ:

1. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
2. For *Name*, enter *From-Branch-to-HQ*.
3. For *Incoming Interface*, select the LAN-side interface (*lan*).
4. For *Outgoing Interface*, select the VPN tunnel interface (*VPN-to-HQ*).
5. For *Source*, select *Branch-original*.
6. For *Destination*, select *HQ-new*.
7. For *Service*, select *ALL*.
8. Enable *NAT*.
9. Select *Use Dynamic IP Pool* and select the *Branch-new* IP pool.

The screenshot shows the configuration for a new firewall policy named "From-Branch-to-HQ". The configuration is as follows:

- Name:** From-Branch-to-HQ
- Incoming Interface:** lan
- Outgoing Interface:** VPN-to-HQ
- Source:** Branch-original
- Destination:** HQ-new
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY (unchecked)
- Inspection Mode:** Flow-based (selected), Proxy-based (unselected)
- Firewall / Network Options:**
  - NAT:** Enabled (toggle is on)
  - IP Pool Configuration:**
    - Use Outgoing Interface Address (unselected)
    - Use Dynamic IP Pool (selected)
    - Selected IP Pool: Branch-new

10. Click **OK**.

### To configure the firewall policy for traffic from HQ to Branch:

1. Click *Create New* and for *Name*, enter *From-HQ-to-Branch*.
2. For *Incoming Interface*, select the VPN tunnel interface (*VPN-to-HQ*).
3. For *Outgoing Interface*, select the LAN-side interface (*lan*).
4. For *Source*, select *HQ-new*.
5. For *Destination*, select the *Branch-new-to-original* VIP.
6. For *Service*, select *ALL*.

## 7. Disable NAT.

Name	From-HQ-to-Branch
Incoming Interface	VPN-to-HQ
Outgoing Interface	lan
Source	HQ-new
Destination	Branch-new-to-original
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based

Firewall / Network Options

NAT ☐

## 8. Click OK.

## To verify the communication across the tunnel:

1. Go to *Dashboard > Network* and click the *IPsec* widget to expand to full screen view. The tunnels should be up on both FortiGates. If you did not enable *Auto-negotiate* in the IPsec VPN settings, you may have to select the tunnel and click *Bring Up*.
2. From a PC on the HQ network, ping a PC on the Branch network using the new IP for the Branch PC. The ping should be successful.

```
C:\Users\jheadley>ping 10.2.2.98

Pinging 10.2.2.98 with 32 bytes of data:
Reply from 10.2.2.98: bytes=32 time=7ms TTL=62
Reply from 10.2.2.98: bytes=32 time=1ms TTL=62
Reply from 10.2.2.98: bytes=32 time=1ms TTL=62
Reply from 10.2.2.98: bytes=32 time=1ms TTL=62

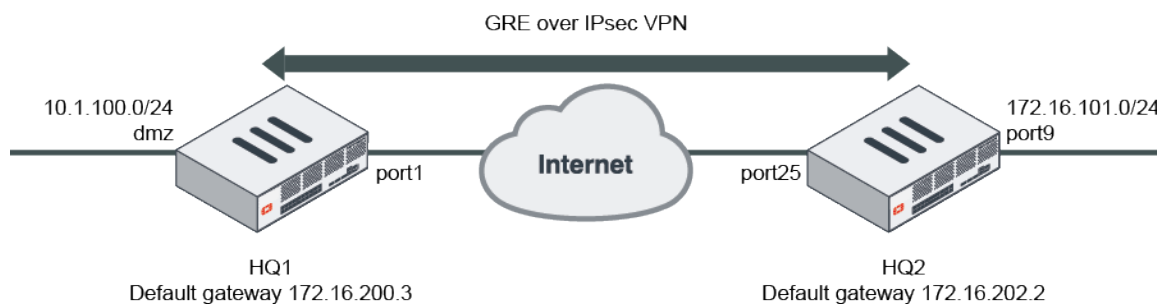
Ping statistics for 10.2.2.98:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 7ms, Average = 2ms
```

3. From a PC on the Branch network, ping a PC on the HQ network using the new IP for the HQ PC. The ping should be successful.

```
[Johns-MacBook-Air:~ John$ ping 10.1.1.12
PING 10.1.1.12 (10.1.1.12): 56 data bytes
64 bytes from 10.1.1.12: icmp_seq=0 ttl=126 time=1.912 ms
64 bytes from 10.1.1.12: icmp_seq=1 ttl=126 time=1.743 ms
64 bytes from 10.1.1.12: icmp_seq=2 ttl=126 time=1.403 ms
64 bytes from 10.1.1.12: icmp_seq=3 ttl=126 time=1.425 ms
^C
--- 10.1.1.12 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.403/1.621/1.912/0.215 ms
```

## GRE over IPsec

This is an example of GRE over an IPsec tunnel using a static route over GRE tunnel and `tunnel-mode` in the `phase2-interface` settings.



### To configure GRE over an IPsec tunnel:

1. Enable subnet overlapping at both HQ1 and HQ2.

```
config system settings
 set allow-subnet-overlap enable
end
```

2. Configure the WAN interface and static route.

#### a. HQ1.

```
config system interface
 edit "port1"
 set ip 172.16.200.1 255.255.255.0
 next
 edit "dmz"
 set ip 10.1.100.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 172.16.200.3
 set device "port1"
 next
end
```

#### b. HQ2.

```
config system interface
 edit "port25"
 set ip 172.16.202.1 255.255.255.0
 next
 edit "port9"
 set ip 172.16.101.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 172.16.202.2
 set device "port25"
```

```
 next
end
```

### 3. Configure IPsec phase1-interface and phase2-interface.

#### a. HQ1.

```
config vpn ipsec phase1-interface
 edit "greipsec"
 set interface "port1"
 set peertype any
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.16.202.1
 set psksecret sample
 next
end
config vpn ipsec phase2-interface
 edit "greipsec"
 set phase1name "greipsec"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
 set protocol 47
 next
end
```

#### b. HQ2.

```
config vpn ipsec phase1-interface
 edit "greipsec"
 set interface "port25"
 set peertype any
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.16.200.1
 set psksecret sample
 next
end
config vpn ipsec phase2-interface
 edit "greipsec"
 set phase1name "greipsec"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
 set protocol 47
 next
end
```

### 4. Configure IPsec tunnel interface IP address.

#### a. HQ1.

```
config system interface
 edit "greipsec"
 set ip 10.10.10.1 255.255.255.255
 set remote-ip 10.10.10.2 255.255.255.255
 next
end
```

#### b. HQ2.

```
config system interface
 edit "greipsec"
```

```
 set ip 10.10.10.2 255.255.255.255
 set remote-ip 10.10.10.1 255.255.255.255
 next
end
```

## 5. Configure the GRE tunnel.

### a. HQ1.

```
config system gre-tunnel
 edit "gre_to_HQ2"
 set interface "greipsec"
 set remote-gw 10.10.10.2
 set local-gw 10.10.10.1
 next
end
```

### b. HQ2.

```
config system gre-tunnel
 edit "gre_to_HQ1"
 set interface "greipsec"
 set remote-gw 10.10.10.1
 set local-gw 10.10.10.2
 next
end
```

## 6. Configure the firewall policy.

### a. HQ1.

```
config firewall policy
 edit 1
 set srcintf "dmz"
 set dstintf "gre_to_HQ2"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set srcintf "gre_to_HQ2"
 set dstintf "dmz"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 3
 set srcintf "greipsec"
 set dstintf "greipsec"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end
```



**b. HQ2.**

```

config firewall policy
 edit 1
 set srcintf "port9"
 set dstintf "gre_to_HQ1"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set srcintf "gre_to_HQ1"
 set dstintf "port9"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 3
 set srcintf "greipsec"
 set dstintf "greipsec"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end

```

**7. Configure the static route.****a. HQ1.**

```

config router static
 edit 2
 set dst 172.16.101.0 255.255.255.0
 set device "gre_to_HQ2"
 next
end

```

**b. HQ2.**

```

config router static
 edit 2
 set dst 10.1.100.0 255.255.255.0
 set device "gre_to_HQ1"
 next
end

```

**To view the VPN tunnel list on HQ1:**

```

diagnose vpn tunnel list
list all ipsec tunnel in vd 0

name=greipsec ver=1 serial=1 172.16.200.1:0->172.16.202.1:0
bound_if=5 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/16 options[0010]=create_dev

```

```

proxyid_num=1 child_num=0 refcnt=12 ilast=19 olast=861 ad=/0
stat: rxp=347 txp=476 rxb=58296 txb=51408
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=8
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=greipsecc proto=47 sa=1 ref=2 serial=2
src: 47:0.0.0.0/0.0.0.0:0
dst: 47:0.0.0.0/0.0.0.0:0
SA: ref=3 options=10226 type=00 soft=0 mtu=1438 expire=41689/0B replaywin=2048
seqno=15c esn=0 replaywin_lastseq=0000015c itn=0
life: type=01 bytes=0/0 timeout=42898/43200
dec: spi=9897bd09 esp=aes key=16 5a60e67bf68379309715bd83931680bf
ah=sha1 key=20 ff35a329056d0d506c0bfc17ef269978a4a57dd3
enc: spi=e362f336 esp=aes key=16 5574acd8587c5751a88950e1bf8fbf57
ah=sha1 key=20 d57ec76ac3c543ac89b2e4d0545518aa2d06669b
dec:pkts/bytes=347/37476, enc:pkts/bytes=347/58296

```

### To view the static routing table on HQ1:

```

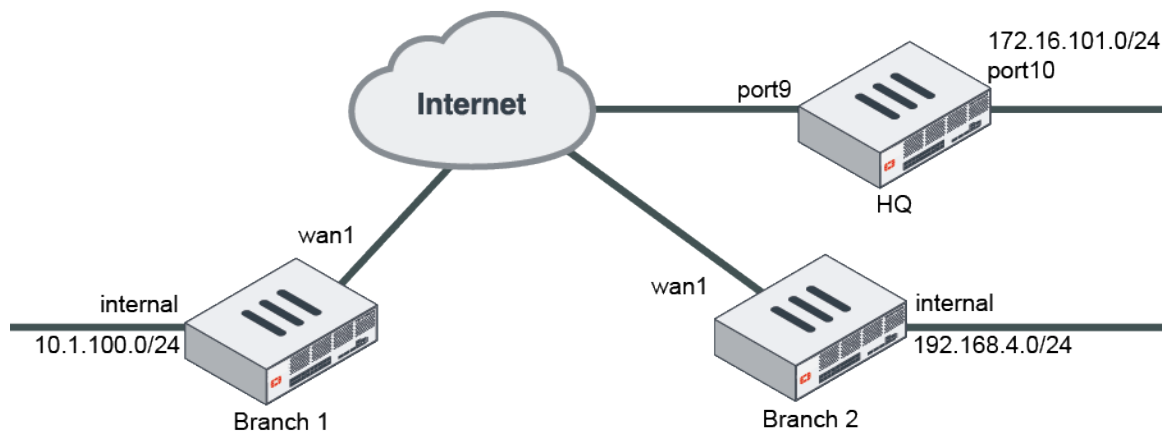
get router info routing-table static
Routing table for VRF=0
S* 0.0.0.0/0 [10/0] via 172.16.200.3, port1
S 172.16.101.0/24 [10/0] is directly connected, gre_to_HQ2

```

## Policy-based IPsec tunnel

This is an example of policy-based IPsec tunnel using site-to-site VPN between branch and HQ. HQ is the IPsec concentrator.

### Sample topology



### Sample configuration

To configure a policy-based IPsec tunnel using the GUI:

- [Configure the IPsec VPN at HQ.](#)
- [Configure the IPsec concentrator at HQ.](#)
- [Configure the firewall policy at HQ.](#)
- [Configure IPsec VPN at branch 1.](#)
- [Configure the firewall policy at branch 1.](#)

- [Configure IPsec VPN at branch 2.](#)
- [Configure the firewall policy at branch 2.](#)

**To configure the IPsec VPN at HQ:**

1. Go to *VPN > IPsec Wizard* to set up branch 1.
  - a. Enter a *VPN Name*. In this example, *to\_branch1*.
  - b. For *Template Type*, click *Custom*. Click *Next*.
  - c. Uncheck *Enable IPsec Interface Mode*.
  - d. For *Remote Gateway*, select *Static IP Address*.
  - e. Enter IP address, in this example, *15.1.1.2*.
  - f. For *Interface*, select *port9*.
  - g. In the *Authentication* section, for *Method*, select *Pre-shared Key* and enter the *Pre-shared Key*.
  - h. Click *OK*.
2. Go to *VPN > IPsec Wizard* to set up branch 2.
  - a. Enter a *VPN Name*. In this example, *to\_branch2*.
  - b. For *Template Type*, click *Custom*. Click *Next*.
  - c. Uncheck *Enable IPsec Interface Mode*.
  - d. For *Remote Gateway*, select *Static IP Address*.
  - e. Enter IP address, in this example, *13.1.1.2*.
  - f. For *Interface*, select *port9*.
  - g. In the *Authentication* section, for *Method*, select *Pre-shared Key* and enter the *Pre-shared Key*.
  - h. Click *OK*.

**To configure the IPsec concentrator at HQ:**

1. Go to *VPN > IPsec Concentrator* and click *Create New*.
2. Enter a name. In this example, *branch*.
3. Add the *Members to\_branch1* and *to\_branch2*.
4. Click *OK*.

**To configure the firewall policy at HQ:**

1. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
2. Enter a policy *Name*.
3. For *Incoming Interface*, select *port10*.
4. For *Outgoing Interface*, select *port9*.
5. Select the *Source*, *Destination*, *Schedule*, *Service*, and set *Action* to *IPsec*.
6. Select the *VPN Tunnel*, in this example, *Branch1/Branch2*.
7. In this example, enable *Allow traffic to be initiated from the remote site*.
8. Click *OK*.

**To configure IPsec VPN at branch 1:**

1. Go to *VPN > IPsec Wizard* to set up branch 1.
2. Enter a VPN name. In this example, *to\_HQ*.
3. For *Template Type*, click *Custom*. Click *Next*.

4. Uncheck *Enable IPsec Interface Mode*.
5. For *Remote Gateway*, select *Static IP Address*.
6. Enter IP address, in this example, *22.1.1.1*.
7. For *Interface*, select *wan1*.
8. In the *Authentication* section, for *Method*, select *Pre-shared Key* and enter the *Pre-shared Key*.
9. Click *OK*.

#### **To configure the firewall policy at branch 1:**

1. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
2. Enter a policy *Name*.
3. Choose the *Incoming Interface*, in this example, *internal*.
4. Choose the *Outgoing Interface*, in this example, *wan1*.
5. Select the *Source*, *Destination*, *Schedule*, *Service*, and set *Action* to *IPsec*.
6. Select the *VPN Tunnel*, in this example, *Branch1/Branch2*.
7. In this example, enable *Allow traffic to be initiated from the remote site*.
8. Click *OK*.

#### **To configure IPsec VPN at branch 2:**

1. Go to *VPN > IPsec Wizard* to set up branch 1.
2. Enter a VPN name. In this example, *to\_HQ*.
3. For *Template Type*, click *Custom*. Click *Next*.
4. Uncheck *Enable IPsec Interface Mode*.
5. For *Remote Gateway*, select *Static IP Address*.
6. Enter IP address, in this example, *22.1.1.1*.
7. For *Interface*, select *wan1*.
8. In the *Authentication* section, for *Method*, select *Pre-shared Key* and enter the *Pre-shared Key*.
9. Click *OK*.

#### **To configure the firewall policy at branch 2:**

1. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
2. Enter a policy *Name*.
3. Choose the *Incoming Interface*, in this example, *internal*.
4. Choose the *Outgoing Interface*, in this example, *wan1*.
5. Select the *Source*, *Destination*, *Schedule*, *Service*, and set *Action* to *IPsec*.
6. Select the *VPN Tunnel*, in this example, *to\_HQ*.
7. In this example, enable *Allow traffic to be initiated from the remote site*.
8. Click *OK*.

#### **To configure a policy-based IPsec tunnel using the CLI:**

1. Configure the HQ WAN interface and static route.

```
config system interface
 edit "port9"
 set alias "WAN"
```

```

 set ip 22.1.1.1 255.255.255.0
 next
 edit "port10"
 set alias "Internal"
 set ip 172.16.101.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 22.1.1.2
 set device "port9"
 next
end

```

## 2. Configure the HQ IPsec phase1 and phase2.

```

config vpn ipsec phase1
 edit "to_branch1"
 set interface "port9"
 set peertype any
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 15.1.1.2
 set psksecret sample
 next
 edit "to_branch2"
 set interface "port9"
 set peertype any
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 13.1.1.2
 set psksecret sample
 next
end
config vpn ipsec phase2
 edit "to_branch1"
 set phase1name "to_branch1"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
 next
 edit "to_branch2"
 set phase1name "to_branch2"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
 next
end

```

## 3. Configure the firewall policy at HQ.

```

config firewall policy
 edit 1
 set srcintf "port10"
 set dstintf "port9"
 set srcaddr "all"
 set dstaddr "10.1.100.0"
 set action ipsec
 set schedule "always"
 set service "ALL"
 set inbound enable
 next
end

```

```
 set vpntunnel "to_branch1"
 next
 edit 2
 set srcintf "port10"
 set dstintf "port9"
 set srcaddr "all"
 set dstaddr "192.168.4.0"
 set action ipsec
 set schedule "always"
 set service "ALL"
 set inbound enable
 set vpntunnel "to_branch2"
 next
end
```

#### 4. Configure the IPsec concentrator at HQ.

```
config vpn ipsec concentrator
 edit "branch"
 set member "to_branch1" "to_branch2"
 next
end
```

#### 5. Configure the branch WAN interface and static route.

##### a. For branch 1.

```
config system interface
 edit "wan1"
 set alias "primary_WAN"
 set ip 15.1.1.2 255.255.255.0
 next
 edit "internal"
 set ip 10.1.100.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 15.1.1.1
 set device "wan1"
 next
end
```

##### b. For branch 2.

```
config system interface
 edit "wan1"
 set alias "primary_WAN"
 set ip 13.1.1.2 255.255.255.0
 next
 edit "internal"
 set ip 192.168.4.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 13.1.1.1
 set device "wan1"
```

```
 next
end
```

## 6. Configure the branch IPsec phase1 and phase2.

### a. For branch 1.

```
config vpn ipsec phase1
 edit "to_HQ"
 set interface "wan1"
 set peertype any
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 22.1.1.1
 set psksecret sample
 next
end
config vpn ipsec phase2
 edit "to_HQ"
 set phase1name "to_HQ"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 next
end
```

### b. For branch 2.

```
config vpn ipsec phase1
 edit "to_HQ"
 set interface "wan1"
 set peertype any
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 22.1.1.1
 set psksecret sample
 next
end
config vpn ipsec phase2
 edit "to_HQ"
 set phase1name "to_HQ"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 next
end
```

## 7. Configure the branch firewall policy.

### a. For branch 1.

```
config firewall policy
 edit 1
 set srcintf "internal"
 set dstintf "wan1"
 set srcaddr "10.1.100.0"
 set dstaddr "all"
 set action ipsec
 set schedule "always"
 set service "ALL"
 set inbound enable
 set vpntunnel "to_HQ"
 next
end
```

**b. For branch 2.**

```

config firewall policy
 edit 1
 set srcintf "internal"
 set dstintf "wan1"
 set srcaddr "192.168.4.0"
 set dstaddr "all"
 set action ipsec
 set schedule "always"
 set service "ALL"
 set inbound enable
 set vpntunnel "to_HQ"
 next
end

```

**To view the IPsec VPN tunnel list at HQ:**

```

diagnose vpn tunnel list

list all ipsec tunnel in vd 0

name=to_branch1 ver=1 serial=4 22.1.1.1:0->15.1.1.2:0
bound_if=42 lgwy=static/1 tun=tunnel/1 mode=auto/1 encap=none/8 options[0008]=npu
proxyid_num=1 child_num=0 refcnt=8 ilast=0 olast=0 ad=/0
stat: rxp=305409 txp=41985 rxb=47218630 txb=2130108
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=to_branch1 proto=0 sa=1 ref=3 serial=1
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0
 SA: ref=6 options=10226 type=00 soft=0 mtu=1438 expire=42604/0B replaywin=2048
 seqno=1 esn=0 replaywin_lastseq=00000680 itn=0
 life: type=01 bytes=0/0 timeout=42932/43200
 dec: spi=ca646442 esp=aes key=16 58c91d4463968ddcccc4fd97de90a4b8
 ah=sha1 key=20 c9176fe2fbc82ef7e726be9ad4af83eb1b55580a
 enc: spi=747c10c4 esp=aes key=16 7cf0f75b784f697bc7f6d8b4bb8a83c1
 ah=sha1 key=20 cdddc376a86f5ca0149346604a59af07a33b11c5
 dec:pkts/bytes=1664/16310, enc:pkts/bytes=0/16354
 npu_flag=03 npu_rgw=15.1.1.2 npu_lgwy=22.1.1.1 npu_selid=3 dec_npuid=2 enc_npuid=2

name=to_branch2 ver=1 serial=5 22.1.1.1:0->13.1.1.2:0
bound_if=42 lgwy=static/1 tun=tunnel/1 mode=auto/1 encap=none/8 options[0008]=npu
proxyid_num=1 child_num=0 refcnt=7 ilast=2 olast=43228 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=to_branch2 proto=0 sa=1 ref=2 serial=1
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0
 SA: ref=3 options=10226 type=00 soft=0 mtu=1280 expire=40489/0B replaywin=2048
 seqno=1 esn=0 replaywin_lastseq=00000000 itn=0
 life: type=01 bytes=0/0 timeout=42931/43200
 dec: spi=ca646441 esp=aes key=16 57ab680d29d4aad4e373579fb50e9909
 ah=sha1 key=20 12a2bc703d2615d917ff544eaff75a6d2c17f1fe
 enc: spi=f9cfff61 esp=aes key=16 3d64da9feb893874e007babce0229259
 ah=sha1 key=20 f92a3ad5e56cb8e89c47af4dac10bf4b4bebf16

```



```
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
npu_flag=00 npu_rgwy=13.1.1.2 npu_lgwy=22.1.1.1 npu_selid=4 dec_npuid=0 enc_npuid=0
```

**To view the IPsec VPN concentrator at HQ:**

```
diagnose vpn concentrator list

list all ipsec concentrator in vd 0
name=branch ref=3 tuns=2 flags=0
```

## FortiGate-to-third-party

This section contains the following topics about FortiGate-to-third-party VPN configurations:

- [IKEv2 IPsec site-to-site VPN to an AWS VPN gateway on page 1171](#)
- [IPsec VPN to Azure with virtual network gateway on page 1177](#)
- [IPsec VPN to an Azure with virtual WAN on page 1188](#)
- [IPSec VPN between a FortiGate and a Cisco ASA with multiple subnets on page 1192](#)
- [Cisco GRE-over-IPsec VPN on page 1193](#)

### IKEv2 IPsec site-to-site VPN to an AWS VPN gateway

This is a sample configuration of an IPsec site-to-site VPN connection between an on-premise FortiGate and an AWS virtual private cloud (VPC).

AWS uses unique identifiers to manipulate a VPN connection's configuration. Each VPN connection is assigned an identifier and is associated with two other identifiers: the customer gateway ID for the FortiGate and virtual private gateway ID.

This example includes the following IDs:

- VPN connection ID: vpn-07e988ccc1d46f749
- Customer gateway ID: cgw-0440c1aebcd2f418a
- Virtual private gateway ID

This example assumes that you have configured VPC-related settings in the AWS management portal as described in [Create and configure your VPC](#).

This example includes creating and configuring two tunnels. You must configure both tunnels on your FortiGate.

**To configure IKEv2 IPsec site-to-site VPN to an AWS VPN gateway:**

1. Configure the first VPN tunnel:
  - a. [Configure Internet Key Exchange \(IKE\)](#).
  - b. [Configure IPsec](#).
  - c. [Configure the tunnel interface](#).
  - d. [Configure border gateway protocol \(BGP\)](#).
  - e. [Configure firewall policies](#).
2. Configure the second VPN tunnel:
  - a. [Configure Internet Key Exchange \(IKE\)](#).
  - b. [Configure IPsec](#).
  - c. [Configure the tunnel interface](#).

- d. [Configure BGP.](#)
- e. [Configure firewall policies.](#)

### To configure IKE for the first VPN tunnel:

A policy is established for the supported ISAKMP encryption, authentication, Diffie-Hellman (DH), lifetime, and key parameters. These sample configurations fulfill the minimum requirements for AES128, SHA1, and DH Group 2. Category VPN connections in the GovCloud AWS region have a minimum requirement of AES128, SHA2, and DH Group 14. To take advantage of AES256, SHA256, or other DH groups such as 14-18, 22, 23, and 24, you must modify these sample configuration files. Higher parameters are only available for VPNs of category "VPN", not for "VPN-Classic".

Your FortiGate's external interface's address must be static. Your FortiGate may reside behind a device performing NAT. To ensure NAT traversal can function, you must adjust your firewall rules to unblock UDP port 4500. If not behind NAT, it is recommended to disable NAT traversal.

Begin configuration in the root VDOM. The interface name must be shorter than 15 characters. It is best if the name is shorter than 12 characters. IPsec dead peer detection (DPD) causes periodic messages to be sent to ensure a security association remains operational.

```
config vpn ipsec phase1-interface
 edit vpn-07e988cccd46f749-0
 set interface "wan1"
 set dpd enable
 set local-gw 35.170.66.108
 set dhgrp 2
 set proposal aes128-sha1
 set keylife 28800
 set remote-gw 3.214.239.164
 set psksecret iCelks0UOob8z4SYMRM6zlx.rU2C3jth
 set dpd-retryinterval 10
 next
end
```

### To configure IPsec for the first VPN tunnel:

The IPsec transform set defines the encryption, authentication, and IPsec mode parameters.

```
config vpn ipsec phase2-interface
 edit "vpn-07e988cccd46f749-0"
 set phase1name "vpn-07e988cccd46f749-0"
 set proposal aes128-sha1
 set dhgrp 2
 set pfs enable
 set keylifeseconds 3600
 next
end
```

### To configure the tunnel interface for the first VPN tunnel:

You must configure a tunnel interface as the logical interface associated with the tunnel. All traffic routed to the tunnel interface must be encrypted and transmitted to the VPC. Similarly, traffic from the VPC will be logically received on this interface.

You must configure the interface's address with your FortiGate's address. If the address changes, you must recreate the FortiGate and VPN connection with Amazon VPC.

The `tcp-mss` option causes the router to reduce the TCP packets' maximum segment size to prevent packet fragmentation.

```
config system interface
 edit "vpn-07e988ccc1d46f749-0"
 set vdom "root"
 set ip 169.254.45.90 255.255.255.255
 set allowaccess ping
 set type tunnel
 set tcp-mss 1379
 set remote-ip 169.254.45.89
 set mtu 1427
 set interface "wan1"
 next
end
```

### To configure BGP for the first VPN tunnel:

BGP is used within the tunnel to exchange prefixes between the virtual private gateway and your FortiGate. The virtual private gateway announces the prefix according to your VPC.

The local BGP autonomous system number (ASN) (65000) is configured as part of your FortiGate. If you must change the ASN, you must recreate the FortiGate and VPN connection with AWS.

Your FortiGate may announce a default route (0.0.0.0/0) to AWS. This is done using a prefix list and route map in FortiOS.

```
config router bgp
 set as 65000
 config neighbor
 edit 169.254.45.89
 set remote-as 64512
 end
 end
end
config router bgp
 config neighbor
 edit 169.254.45.89
 set capability-default-originate enable
 end
 end
end
config router prefix-list
 edit "default_route"
 config rule
 edit 1
 set prefix 0.0.0.0 0.0.0.0
 next
 end
 end
end
config router route-map
 edit "routemap1"
 config rule
 edit 1
```

```
 set match-ip-address "default_route"
 next
end
next
end
```

To advertise additional prefixes to the Amazon VPC, add these prefixes to the network statement and identify the prefix you want to advertise. Ensure that the prefix is present in the routing table of the device with a valid next-hop. If you want to advertise 192.168.0.0/16 to Amazon, you would do the following:

```
config router bgp
config network
 edit 1
 set prefix 192.168.0.0 255.255.0.0
 next
end
```

### To configure firewall policies for the first VPN tunnel:

Create a firewall policy permitting traffic from your local subnet to the VPC subnet, and vice-versa.

This example policy permits all traffic from the local subnet to the VPC. First, view all existing policies using the `show firewall policy` command. Then, create a new firewall policy starting with the next available policy ID. In this example, running `show firewall policy` displayed policies 1, 2, 3, and 4, so you would proceed to create policy 5.

```
config firewall policy
 edit 5
 set srcintf "vpn-07e988cccd46f749-0"
 set dstintf internal
 set srcaddr all
 set dstaddr all
 set action accept
 set schedule always
 set service ANY
 next
end
config firewall policy
 edit 5
 set srcintf internal
 set dstintf "vpn-07e988cccd46f749-0"
 set srcaddr all
 set dstaddr all
 set action accept
 set schedule always
 set service ANY
 next
end
```

### To configure IKE for the second VPN tunnel:

A policy is established for the supported ISAKMP encryption, authentication, DH, lifetime, and key parameters. These sample configurations fulfill the minimum requirements for AES128, SHA1, and DH Group 2. Category VPN connections in the GovCloud AWS region have a minimum requirement of AES128, SHA2, and DH Group 14. To take advantage of AES256, SHA256, or other DH groups such as 14-18, 22, 23, and 24, you must modify these sample configuration files. Higher parameters are only available for VPNs of category "VPN", not for "VPN-Classic".

Your FortiGate's external interface's address must be static. Your FortiGate may reside behind a device performing NAT. To ensure NAT traversal can function, you must adjust your firewall rules to unblock UDP port 4500. If not behind NAT, it is recommended to disable NAT traversal.

Begin configuration in the root VDOM. The interface name must be shorter than 15 characters. It is best if the name is shorter than 12 characters. IPsec DPD causes periodic messages to be sent to ensure a security association remains operational.

```
config vpn ipsec phase1-interface
 edit vpn-07e988cccl46f749-1
 set interface "wan1"
 set dpd enable
 set local-gw 35.170.66.108
 set dhgrp 2
 set proposal aes128-sha1
 set keylife 28800
 set remote-gw 100.25.187.58
 set psksecret IjFzyDneUtDdAT4RNmQ85apUG3y4Akre
 set dpd-retryinterval 10
 next
end
```

### To configure IPsec for the second VPN tunnel:

The IPsec transform set defines the encryption, authentication, and IPsec mode parameters.

```
config vpn ipsec phase2-interface
 edit "vpn-07e988cccl46f749-1"
 set phasename "vpn-07e988cccl46f749-1"
 set proposal aes128-sha1
 set dhgrp 2
 set pfs enable
 set keylifeseconds 3600
 next
end
```

### To configure the tunnel interface for the second VPN tunnel:

You must configure a tunnel interface as the logical interface associated with the tunnel. All traffic routed to the tunnel interface must be encrypted and transmitted to the VPC. Similarly, traffic from the VPC will be logically received on this interface.

You must configure the interface's address with your FortiGate's address. If the address changes, you must recreate the FortiGate and VPN connection with Amazon VPC.

The `tcp-mss` option causes the router to reduce the TCP packets' maximum segment size to prevent packet fragmentation.

```
config system interface
 edit "vpn-07e988cccl46f749-1"
 set vdom "root"
 set ip 169.254.44.162 255.255.255.255
 set allowaccess ping
 set type tunnel
 set tcp-mss 1379
 set remote-ip 169.254.44.161
 set mtu 1427
 set interface "wan1"
```

```
 next
end
```

### To configure BGP for the second VPN tunnel:

BGP is used within the tunnel to exchange prefixes between the virtual private gateway and your FortiGate. The virtual private gateway announces the prefix according to your VPC.

The local BGP ASN (65000) is configured as part of your FortiGate. If you must change the ASN, you must recreate the FortiGate and VPN connection with AWS.

Your FortiGate may announce a default route (0.0.0.0/0) to AWS. This is done using a prefix list and route map in FortiOS.

```
config router bgp
 set as 65000
 config neighbor
 edit 169.254.44.161
 set remote-as 64512
 end
 end
config router bgp
 config neighbor
 edit 169.254.44.161
 set capability-default-originate enable
 end
 end
config router prefix-list
 edit "default_route"
 config rule
 edit 1
 set prefix 0.0.0.0 0.0.0.0
 next
 end
 end
end
config router route-map
 edit "routemap1"
 config rule
 edit 1
 set match-ip-address "default_route"
 next
 end
 next
end
```

To advertise additional prefixes to the Amazon VPC, add these prefixes to the network statement and identify the prefix you want to advertise. Ensure that the prefix is present in the routing table of the device with a valid next-hop. If you want to advertise 192.168.0.0/16 to Amazon, you would do the following:

```
config router bgp
config network
 edit 1
 set prefix 192.168.0.0 255.255.0.0
 next
end
```

**To configure firewall policies for the second VPN tunnel:**

Create a firewall policy permitting traffic from your local subnet to the VPC subnet, and vice-versa.

This example policy permits all traffic from the local subnet to the VPC. First, view all existing policies using the `show firewall policy` command. Then, create a new firewall policy starting with the next available policy ID. In this example, running `show firewall policy` displayed policies 1, 2, 3, 4, and 5, so you would proceed to create policy 6.

```
config firewall policy
 edit 6
 set srcintf "vpn-07e988cccd46f749-1"
 set dstintf internal
 set srcaddr all
 set dstaddr all
 set action accept
 set schedule always
 set service ANY
 next
end
config firewall policy
 edit 6
 set srcintf internal
 set dstintf "vpn-07e988cccd46f749-1"
 set srcaddr all
 set dstaddr all
 set action accept
 set schedule always
 set service ANY
 next
end
```

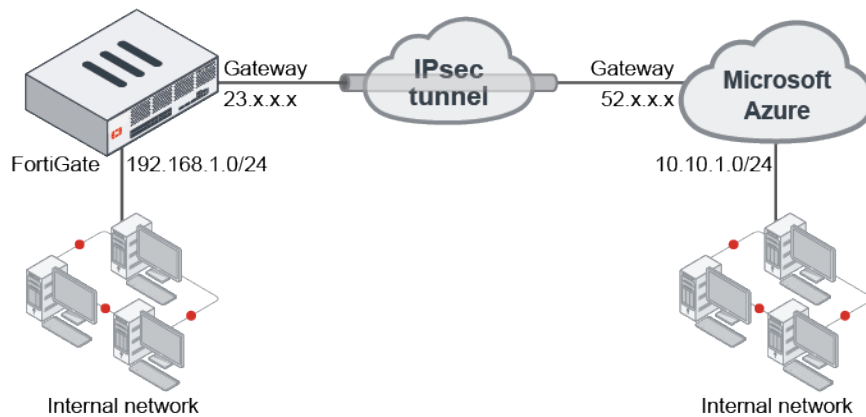
**IPsec VPN to Azure with virtual network gateway**

This example shows how to configure a site-to-site IPsec VPN tunnel to Microsoft Azure. It shows how to configure a tunnel between each site, avoiding overlapping subnets, so that a secure tunnel can be established.

**Prerequisites**

- A FortiGate with an Internet-facing IP address
- A valid Microsoft Azure account

## Sample topology



## Sample configuration

This sample configuration shows how to:

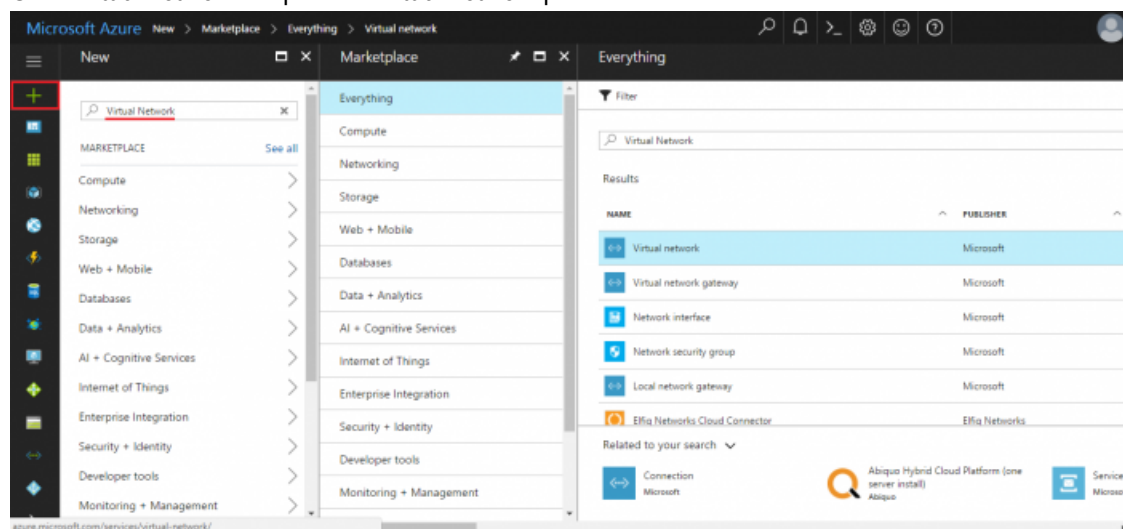
1. [Configure an Azure virtual network.](#)
2. [Specify the Azure DNS server.](#)
3. [Configure the Azure virtual network gateway.](#)
4. [Configure the Azure local network gateway.](#)
5. [Configure the FortiGate tunnel.](#)
6. [Create the Azure firewall object.](#)
7. [Create the FortiGate firewall policies.](#)
8. [Create the FortiGate static route.](#)
9. [Create the Azure site-to-site VPN connection.](#)
10. [Check the results.](#)

### To configure an Azure virtual network:

1. Log in to Azure and click *New*.
2. In *Search the Marketplace*, type *Virtual network*.



3. Click *Virtual network* to open the *Virtual network* pane.



4. At the bottom of the *Virtual network* pane, click the *Select a deployment model* dropdown list and select *Resource Manager*.
5. Click *Create*.

**Virtual network**  
 Microsoft

Create a logically isolated section in Microsoft Azure with this networking service. You can securely connect it to your on-premises datacenter or a single client machine using an IPsec connection. Virtual Networks make it easy for you to take advantage of the scalable, on-demand infrastructure of Azure while providing connectivity to data and applications on-premises, including systems running on Windows Server, mainframes, and UNIX.

Use Virtual Network to:

- Extend your datacenter
- Build distributed applications
- Remotely debug your applications

PUBLISHER	Microsoft
USEFUL LINKS	<a href="#">Service overview</a>
	<a href="#">Documentation</a>
	<a href="#">Pricing</a>

Select a deployment model ⓘ

Resource Manager ▼

**Create**

6. On the *Create virtual network* pane, enter your virtual network settings, and click *Create*.

**Create virtual network**

\* Name  
kleroux\_VPN ✓

\* Address space ⓘ  
10.10.0.0/16 ✓  
10.10.0.0 - 10.10.255.255 (65536 addresses)

\* Subnet name  
default

\* Subnet address range ⓘ  
10.10.0.0/24 ✓  
10.10.0.0 - 10.10.0.255 (256 addresses)

\* Subscription  
Free Trial ▼

\* Resource group ⓘ  
☒ Create new ☐ Use existing  
techdocs ✓

\* Location  
Canada East ▼

**Create**

### To specify the Azure DNS server:

1. Open the virtual network you just created.
2. Click *DNS servers* to open the *DNS servers* pane.
3. Enter the IP address of the DNS server and click *Save*.

**kleroux\_VPN - DNS servers**  
Virtual network

Search (Ctrl+*/*)

Save Discard

Virtual machines within this virtual network must be restarted to utilize the updated DNS server settings.

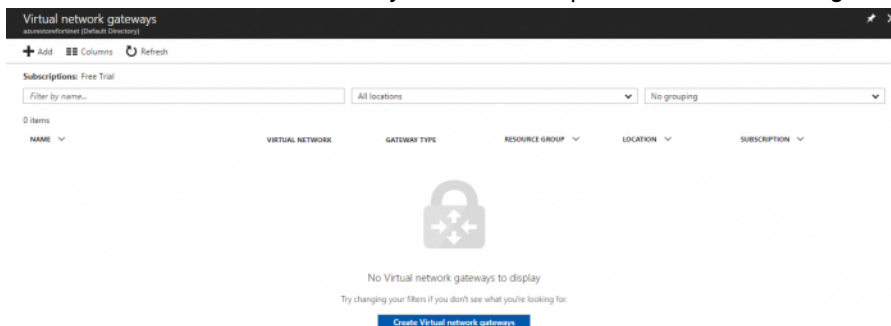
DNS servers ⓘ  
☐ Default (Azure-provided)  
☒ Custom

8.8.8.8 ...  
Add... ..

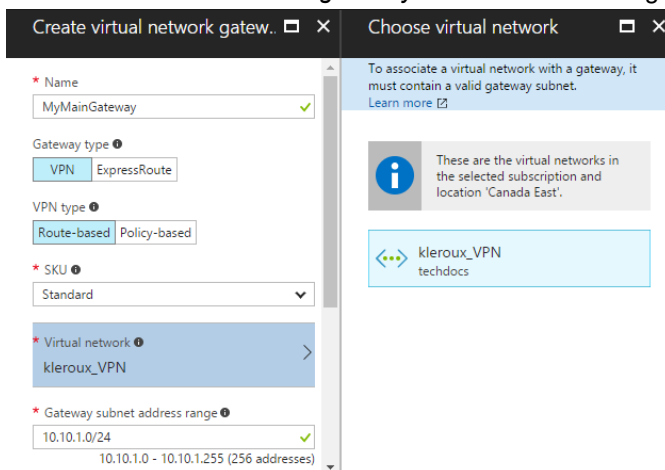
Overview  
Activity log  
Access control (IAM)  
Tags  
SETTINGS  
Address space  
Connected devices  
Subnets  
DNS servers

### To configure the Azure virtual network gateway:

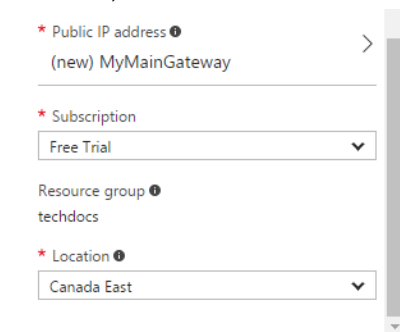
1. In the portal dashboard, go to *New*.
2. Search for *Virtual Network Gateway* and click it to open the *Virtual network gateway* pane.



3. Click *Create Virtual network gateways* and enter the settings for your virtual network gateway.



4. If needed, create a Public IP address.



☐ Pin to dashboard

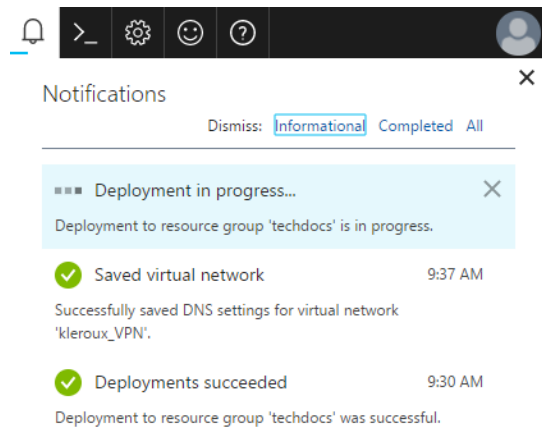
**Create**

[Automation options](#)

Provisioning a virtual network gateway may take up to 45 minutes.

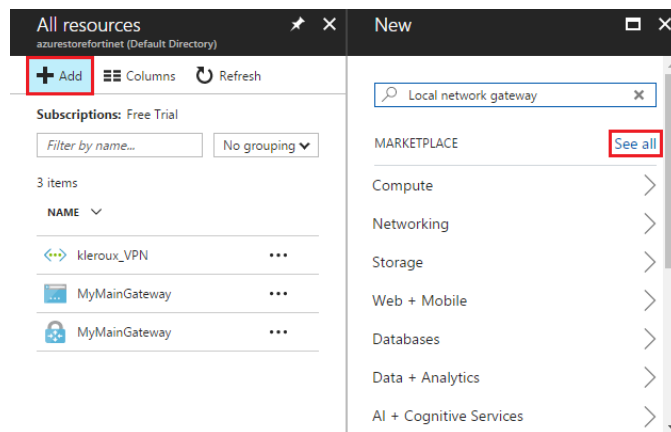
5. Click *Create*.

Creating the virtual network gateway might take some time. When the provisioning is done, you'll receive a notification.

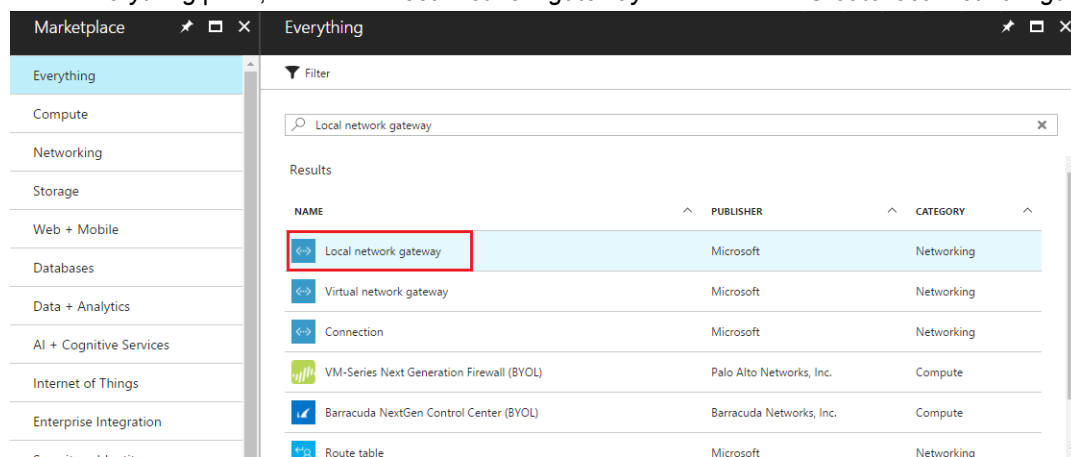


### To configure the Azure local network gateway:

1. In the portal dashboard, click *All resources*.
2. Click *Add* and then click *See all*.



3. In the *Everything* pane, search for *Local network gateway* and then click *Create local network gateway*.



4. For the *IP address*, enter the local network gateway IP address, that is, the FortiGate's external IP address.

**Create local network gateway** [X]

\* Name  
MyVirtualNetworkLocalNet ✓

\* IP address ⓘ  
24 ✓

Address space ⓘ  
192.168.1.0/24 ...  
Add additional address range ...

\* Subscription  
Free Trial ▼

\* Resource group ⓘ  
☐ Create new ☒ Use existing  
techdocs ▼

\* Location  
Canada East ▼

☐ Pin to dashboard

**Create** [Automation options](#)

5. Set the remaining values for your local network gateway and click *Create*.

### To configure the FortiGate tunnel:

1. In the FortiGate, go to *VPN > IP Wizard*.
2. Enter a *Name* for the tunnel, click *Custom*, and then click *Next*.

**1 VPN Setup**

Name  
ToAzureVPN

Template Type  
Site to Site Remote Access **Custom**

3. Configure the *Network* settings.
  - For *Remote Gateway*, select *Static IP Address* and enter the IP address provided by Azure.
  - For *Interface*, select *wan1*.
  - For *NAT Traversal*, select *Disable*,
  - For *Dead Peer Detection*, select *On Idle*.
  - In the *Authentication* section, select
4. Configure the *Authentication* settings.
  - For *Method*, select *Pre-shared Key* and enter the *Pre-shared Key*.
  - For *IKE*, select *2*.

Network	
IP Version	<b>IPv4</b> IPv6
Remote Gateway	Static IP Address
IP Address	52. [redacted]
Interface	wan1
Mode Config	<input type="checkbox"/>
NAT Traversal	Enable <b>Disable</b> Forced
Dead Peer Detection	Disable <b>On Idle</b> On Demand
Authentication	
Method	Pre-shared Key
Pre-shared Key	••••••••
IKE	
Version	1 <b>2</b>
Peer Options	
Accept Types	Any peer ID

5. Configure the *Phase 1 Proposal* settings.

- Set the Encryption and Authentication combination to the three supported encryption algorithm combinations accepted by Azure.
  - AES256 and SHA1
  - 3DES and SHA1
  - AES256 and SHA256
- For *Diffie-Hellman Groups*, select 2.
- Set *Key Lifetime (seconds)* to 28800.

Phase 1 Proposal		<a href="#">Add</a>
Encryption	AES256	Authentication SHA1 <input type="checkbox"/>
Encryption	3DES	Authentication SHA1 <input type="checkbox"/>
Encryption	AES256	Authentication SHA256 <input type="checkbox"/>
Diffie-Hellman Group	<input type="checkbox"/> 30 <input type="checkbox"/> 29 <input type="checkbox"/> 28 <input type="checkbox"/> 27 <input type="checkbox"/> 21 <input type="checkbox"/> 20 <input type="checkbox"/> 19 <input type="checkbox"/> 18 <input type="checkbox"/> 17 <input type="checkbox"/> 16 <input type="checkbox"/> 15 <input type="checkbox"/> 14 <input type="checkbox"/> 5 <input checked="" type="checkbox"/> <b>2</b> <input type="checkbox"/> 1	
Key Lifetime (seconds)	28800	
Local ID		

6. In *Phase 2 Selectors*, expand the *Advanced* section to configure the *Phase 2 Proposal* settings.

- Set the Encryption and Authentication combinations.
  - AES256 and SHA1
  - 3DES and SHA1
  - AES256 and SHA256
- Uncheck *Enable Perfect Forward Secrecy (PFS)*.
- Set *Key Lifetime (seconds)* to 27000.

Phase 2 Selectors

Name	Local Address	Remote Address
ToAzureVPN	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2

Name: ToAzureVPN

Comments:

Local Address: Subnet 0.0.0.0/0.0.0.0

Remote Address: Subnet 0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal

Encryption	AES256	Authentication	SHA1	<input type="button" value="X"/>
Encryption	3DES	Authentication	SHA1	<input type="button" value="X"/>
Encryption	AES256	Authentication	SHA256	<input type="button" value="X"/>

Enable Replay Detection ☐

Enable Perfect Forward Secrecy (PFS) ☐

Local Port: All ☒

Remote Port: All ☒

Protocol: All ☒

Auto-negotiate ☐

Autokey Keep Alive ☐

Key Lifetime: Seconds

Seconds: 27000

7. Click OK.

### To create the Azure firewall object:

1. In the FortiGate, go to *Policy & Objects > Addresses*.
2. Create a firewall object for the Azure VPN tunnel.

### To create the FortiGate firewall policies:

1. In the FortiGate, go to *Policy & Objects > IPv4 Policy*.
2. Create a policy for the site-to-site connection that allows outgoing traffic.
  - Set the *Source* address and *Destination* address using the firewall objects you just created.
  - Disable *NAT*.

Name	ToAzureVPN
Incoming Interface	internal
Outgoing Interface	ToAzureVPN
Source	all
Destination	AzureNetwork
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN <input type="checkbox"/> IPsec

Firewall / Network Options

NAT ☐

3. Create another policy that allows incoming traffic.
  - For this policy, reverse the *Source* address and *Destination* address.

Name	FromAzureVPN
Incoming Interface	ToAzureVPN
Outgoing Interface	internal
Source	AzureNetwork
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN <input type="checkbox"/> IPsec

Firewall / Network Options

NAT ☐

4. We recommend limiting the TCP maximum segment size (MSS) being sent and received so as to avoid packet drops and fragmentation.



To do this, use the following CLI commands on both policies.

```
config firewall policy
 edit <policy-id>
 set tcp-mss-sender 1350
 set tcp-mss-receiver 1350
 next
end
```

### To create the FortiGate static route:

1. In the FortiGate, go to *Network > Static Routes*.
2. Create an IPv4 Static Route that forces outgoing traffic going to Azure to go through the route-based tunnel.
3. Set the *Administrative Distance* to a value lower than the existing default route value.

Destination ⓘ	Subnet	Named Address	Internet Service
	10.10.0.0/16		
Device	ToAzureVPN ▼		
Administrative Distance ⓘ	2		
Comments			
Status	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Disabled		

### To create the Azure site-to-site VPN connection:

1. In the Azure portal, locate and select your virtual network gateway.
2. In the *Settings* pane, click *Connections* and then click *Add*.

The screenshot shows the Azure portal interface. On the left, under 'All resources', there's a list of subscriptions. 'MyMainGateway' is selected. On the right, the 'MyMainGateway' settings page is open, and the 'Connections' tab is active. The 'Connections' section shows a list of connections, with 'MyMainGateway' highlighted. The 'Settings' pane on the right shows various options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Configuration, Connections, Point-to-site configuration, Properties, Locks, and Automation script.

3. Enter the settings for your connection. Ensure the *Shared Key (PSK)* matches the *Pre-shared Key* for the FortiGate tunnel.

## To check the results:

1. In the FortiGate, go to *Monitor > IPsec Monitor*.

- Check that the tunnel is up.

Refresh

Reset Statistics

Bring Up

Bring Down

Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 1
ToAzureVPN	Custom	52.		Up			ToAzureVPN

- If the tunnel is down, right-click the tunnel and select *Bring Up*.

Refresh	Reset Statistics	Bring Up	Bring Down				
Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing Data	Phase 1
ToAzureVPN	Custom	52. [REDACTED]		Down			ToAzureVPN

Reset Statistics  
 Bring Up  
 Bring Down

2. In the FortiGate, go to *Log & Report > Events*.

- Select an event to view more information and verify the connection.

3. In the Azure portal dashboard, click *All resources* and locate your virtual network gateway.

- a. In your virtual network gateway pane, click *Connections* to see the status of each connection.

- b. Click a connection to open the *Essentials* pane to view more information about that connection.

- If the connection is successful, the *Status* shows *Connected*.
- See the *ingress* and *egress* bytes to confirm traffic flowing through the tunnel.

## IPsec VPN to an Azure with virtual WAN

This is a sample configuration of an IPsec site-to-site VPN connection between an on-premise FortiGate and an Azure virtual network (VNet). This example uses Azure virtual WAN (vWAN) to establish the VPN connection.



- Azure must use IPsec v2 for this configuration.
- Azure uses overlapped subnet IP addresses for the IPsec interfaces.

## To configure IKEv2 IPsec site-to-site VPN to an Azure VPN gateway:

1. In the Azure management portal, configure vWAN-related settings as described in [Tutorial: Create a Site-to-Site connection using Azure Virtual WAN](#).

If a custom BGP IP address is configured on Azure's vWAN, such as 169.254.21.6 and 169.254.21.7, you must configure the FortiGate `remote-IP` to the corresponding *Custom BGP IP Address* value. If a custom BGP IP address is not configured, FortiGate `remote-IPs` should point to the *Default BGP IP Address* value.

2. Download the VPN configuration. The following shows an example VPN configuration:

```
[{"configurationVersion":{"LastUpdatedTime":"2019-07-16T22:16:28.0409002Z","Version":"be5c5787-b903-43b1-a237-49eae1b373e4"},"vpnSiteConfiguration":{"Name":"toaws","IPAddress":"3.220.252.93","BgpSetting":{"Asn":7225,"BgpPeeringAddress":"169.254.24.25","PeerWeight":32768},"LinkName":"toaws"},"vpnSiteConnections":[{"hubConfiguration":{"AddressSpace":"10.1.0.0/16","Region":"West US","ConnectedSubnets":["10.2.0.0/16"]},"gatewayConfiguration":{"IpAddresses":{"Instance0":"52.180.90.47","Instance1":"52.180.89.94"},"BgpSetting":{"Asn":65515,"BgpPeeringAddresses":{"Instance0":"10.1.0.7","Instance1":"10.1.0.6"},"PeerWeight":0},"connectionConfiguration":{"IsBgpEnabled":true,"PSK":"Fortinet123#","IPsecParameters":{"SADataSizeInKilobytes":102400000,"SALifeTimeInSeconds":3600}}}}] }
```

3. Configure the following on the FortiGate. Note for `set proposal`, you can select from several proposals.

```
config vpn ipsec phase1-interface
```

```
edit "toazure1"
```

```
set interface "port1"
```

```
set ike-version 2
```

```
set keylife 28800
```

```
set peertype any
```

```
set proposal aes256-sha1
```

```
set dhgrp 2
```

```
set remote-gw 52.180.90.47
```

```
set psksecret ENC
```

```
BJeE+CnBFbdepvMMfXmblQlWmB/QfxAvSuj0/Ol3KI3LgP0ac1Rc80YJRHn2Q7ocGpF96/7F0MCN
RjAEk62wQHeHni8zQKc0DGTffRIyf/ln6l3JMp+r2hVFTv4lHlzfKlE5L+rOuSPj4y94lrJVPjIx9
aID7dAYUMUh/DlelTB/PqAXAt
```

```
0JU+9gDbki4br5Zq8tQ==
```

```
next
```

```
edit "toazure2"
```

```
set interface "port1"
```

```
set ike-version 2
```

```
set keylife 28800
```

```
set peertype any
```

```
set proposal aes256-sha1
```

```
set dhgrp 2
```

```
set remote-gw 52.180.89.94
```

```
set psksecret ENC
```

```
sNVpQEGX79oH3u57I6AjiPdPALYIERj7CMDSJY7RG39g0yUmPVJVcq1+u5v3gA6URhzaD3NjqUoIf
JD3yOE34mIWfo9Q6skowGnQURlQxukENC8kTpEl3YqYESCKULoRc3/sVKDZItYjWcZ/0iHsqkCyWv
m/jDJuy3UPxI7uOktkDtZPho8
```

```
wjnMYeKmMR5EaG28oSA==
```

```
next
```

```
end
config vpn ipsec phase2-interface
 edit "toazure1"
 set phase1name "toazure1"
 set proposal aes256-sha1
 set dhgrp 2
 set keylifeseconds 3600
 next
 edit "toazure2"
 set phase1name "toazure2"
 set proposal aes256-sha1
 set dhgrp 2
 set keylifeseconds 3600
 next
end
config system settings
 set allow-subnet-overlap enable
end
config system interface
 edit "toazure1"
 set vdom "root"
 set ip 169.254.24.25 255.255.255.255
 set type tunnel
 set remote-ip 10.1.0.7 255.255.255.255
 set snmp-index 4
 set interface "port1"
 next
 edit "toazure2"
 set vdom "root"
 set ip 169.254.24.25 255.255.255.255
 set type tunnel
 set remote-ip 10.1.0.6 255.255.255.255
 set snmp-index 5
 set interface "port1"
 next
end
config router bgp
 set as 7225
 set router-id 169.254.24.25
 config neighbor
 edit "10.1.0.7"
 set remote-as 65515
 next
 edit "10.1.0.6"
 set remote-as 65515
 next
 end
config network
 edit 1
 set prefix 172.30.101.0 255.255.255.0
 next
end
config redistribute "connected"
 set status enable
end
config redistribute "rip"
end
```

```

 config redistribute "ospf"
 end
 config redistribute "static"
 end
 config redistribute "isis"
 end
 config redistribute6 "connected"
 end
 config redistribute6 "rip"
 end
 config redistribute6 "ospf"
 end
 config redistribute6 "static"
 end
 config redistribute6 "isis"
 end
end

```

4. Run `diagnose vpn tunnel list`. If the configuration was successful, the output should resemble the following:

```

name=toazure1 ver=2 serial=3 172.30.1.83:4500->52.180.90.47:4500
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refcnt=15 ilast=16 olast=36 ad=/0
stat: rxp=41 txp=41 rxb=5104 txb=2209
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=keepalive draft=0 interval=10 remote_port=4500
proxyid=toazure1 proto=0 sa=1 ref=2 serial=4
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0
 SA: ref=3 options=10226 type=00 soft=0 mtu=8926 expire=2463/0B replaywin=2048
 seqno=2a esn=0 replaywin_lastseq=00000029 itn=0
 life: type=01 bytes=0/0 timeout=3300/3600
 dec: spi=c13f7928 esp=aes key=32
009a86bb0d6f5fee66af7b8232c8c0f22e6ec5c61ba19c93569bd0cd115910a9
 ah=sha1 key=20 f05bfeb0060afa89d4afdfac35960a8a7a4d4856
 enc: spi=b40a6c70 esp=aes key=32
ale361075267ba72b39924c5e6c766fd0b08e0548476de2792ee72057fe60d1d
 ah=sha1 key=20 b1d24bedb0eb8fbd26de3e7c0b0a3a799548f52f
 dec:pkts/bytes=41/2186, enc:pkts/bytes=41/5120

name=toazure2 ver=2 serial=4 172.30.1.83:4500->52.180.89.94:4500
bound_if=3 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refcnt=16 ilast=16 olast=16 ad=/0
stat: rxp=40 txp=40 rxb=4928 txb=2135
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=keepalive draft=0 interval=10 remote_port=4500
proxyid=toazure2 proto=0 sa=1 ref=2 serial=4
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0
 SA: ref=3 options=10626 type=00 soft=0 mtu=8926 expire=2427/0B replaywin=2048
 seqno=29 esn=0 replaywin_lastseq=00000028 itn=0
 life: type=01 bytes=0/0 timeout=3299/3600
 dec: spi=c13f791d esp=aes key=32
759898cbb77afe448116b1fb0fb6d2f0eb99621ea6ed8dd4417ffdb901eb82be
 ah=sha1 key=20 533ec5dc8a1910221e7742b12f9de1b41205622c
 enc: spi=67934bfe esp=aes key=32

```

```
9b5710bfb4ba784722241ec371ba8066629febcd75da6f8471915bdeb874ca80
 ah=sha1 key=20 5099fed7edac2b960294094f1a8188ab42f34d7b
 dec:pkts/bytes=40/2087, enc:pkts/bytes=40/4976
```

Routing table for VRF=0

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP

O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default

```
S* 0.0.0.0/0 [5/0] via 172.30.1.1, port1
B 10.1.0.0/16 [20/0] via 10.1.0.6, toazure2, 00:15:01
C 10.1.0.6/32 is directly connected, toazure2
C 10.1.0.7/32 is directly connected, toazure1
B 10.2.0.0/16 [20/0] via 10.1.0.6, toazure2, 00:15:01
C 169.254.24.25/32 is directly connected, toazure1
 is directly connected, toazure2
C 172.30.1.0/24 is directly connected, port1
C 172.30.101.0/24 is directly connected, port2
```

## IPSec VPN between a FortiGate and a Cisco ASA with multiple subnets

When a Cisco ASA unit has multiple subnets configured, multiple phase 2's must be created on the FortiGate, and not just multiple subnets.

This is because the FortiGate uses the same SPI value to bring up the phase 2 for all of the subnets, while the Cisco ASA expects different SPI values for each of its configured subnets. Using multiple phase 2's on the FortiGate creates different SPI values for each subnet.

### To configure multiple phase 2 interfaces in route-based mode:

```
config vpn ipsec phase2-interface
 edit "First subnet"
 set phasename "VPN to Cisco"
 set src-subnet 192.168.227.253 255.255.255.255
 set dst-subnet 10.142.0.0 255.255.254.0
 next
 edit "Second subnet"
 set phasename "VPN to Cisco"
 set src-subnet 192.168.227.253 255.255.255.255
 set dst-subnet 10.143.0.0 255.255.254.0
 next
end
```

### To configure multiple phase 2 interfaces in policy-based mode:

```
config vpn ipsec phase2
 edit "First subnet"
 set phasename "VPN to Cisco"
 set src-subnet 192.168.227.253 255.255.255.255
 set dst-subnet 10.142.0.0 255.255.254.0
```

```

next
edit "Second subnet"
 set phasename "VPN to Cisco"
 set src-subnet 192.168.227.253 255.255.255.255
 set dst-subnet 10.143.0.0 255.255.254.0
next
end

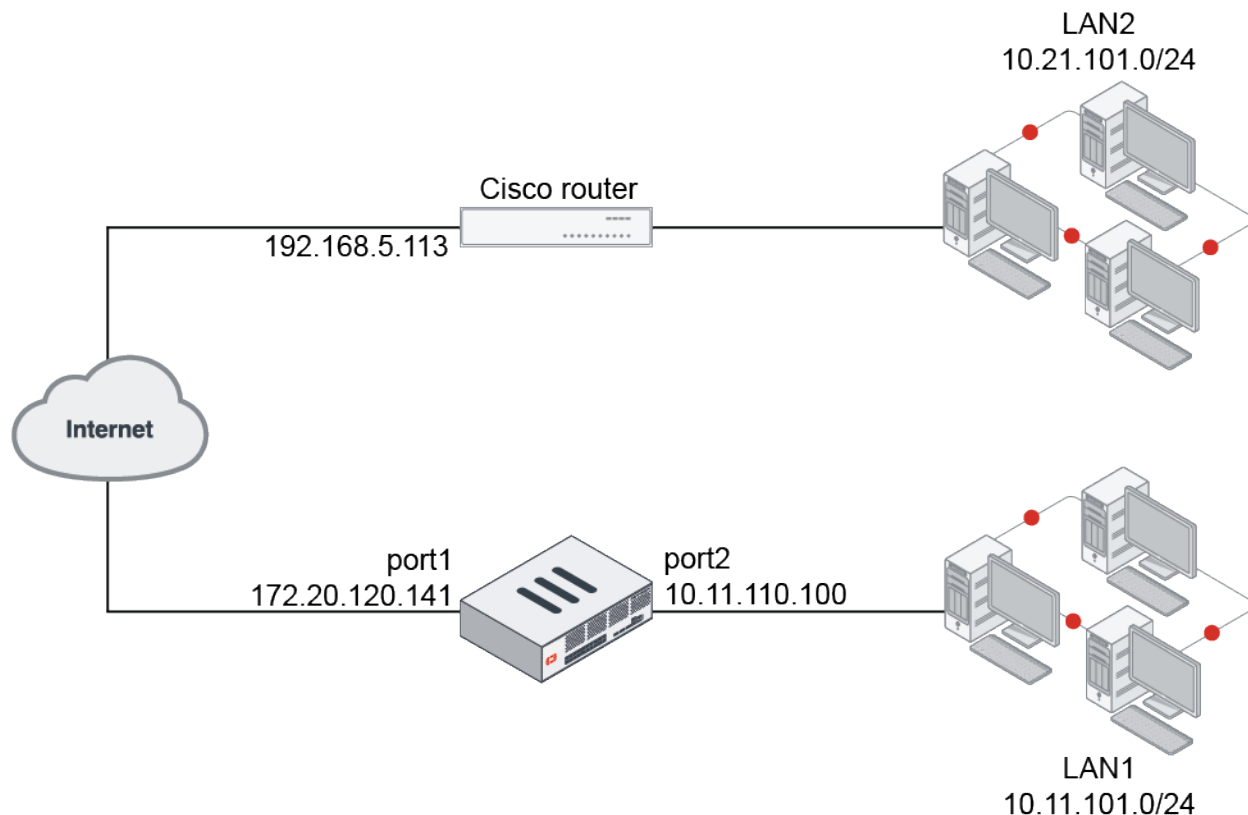
```

## Cisco GRE-over-IPsec VPN

This is a sample configuration of a FortiGate VPN that is compatible with Cisco-style VPNs that use GRE in an IPsec tunnel. Cisco products with VPN support often use the GRE protocol tunnel over IPsec encryption. Cisco VPNs can use either transport mode or tunnel mode IPsec.

### Topology

In this example, LAN1 users are provided with access to LAN2.



### Configuring the FortiGate

There are five steps to configure GRE-over-IPsec with a FortiGate and Cisco router:

1. [Enable overlapping subnets.](#)
2. [Configure a route-based IPsec VPN on the external interface.](#)
3. [Configure a GRE tunnel on the virtual IPsec interface.](#)
4. [Configure security policies.](#)
5. [Configure the static route.](#)

## Enabling overlapping subnets

Overlapping subnets are required because the IPsec and GRE tunnels will use the same addresses. By default, each FortiGate network interface must be on a separate network. This configuration assigns an IPsec tunnel endpoint and the external interface to the same network.

### To enable overlapping subnets:

```
config system settings
 set allow-subnet-overlap enable
next
end
```

## Configuring a route-based IPsec VPN

A route-based VPN that use encryption and authentication algorithms compatible with the Cisco router is required. Pre-shared key authentication is used in this configuration.

### To configure route-based IPsec in the GUI:

1. Go to *VPN > IPsec Wizard* and select the *Custom* template.
2. Enter the tunnel name (*tocisco*) and click *Next*.
3. Enter the following:

<b>Remote Gateway</b>	Static IP Address
<b>IP Address</b>	Cisco router public interface (192.168.5.113)
<b>Interface</b>	FortiGate public interface (172.20.120.141)
<b>Authentication Method</b>	Pre-shared Key
<b>Pre-shared Key</b>	Entry must match the pre-shared key on the Cisco router
<b>Mode</b>	Main (ID Protection)
<b>Phase 1 Proposal</b>	3DES-SHA1, AES128-SHA1 (at least one proposal must match the settings on the Cisco router)
<b>Local Address</b>	GRE local tunnel endpoint IP address (172.20.120.141)
<b>Remote Address</b>	GRE remote tunnel endpoint IP address (192.168.5.113)
<b>Phase 2 Proposal</b>	3DES-MD5 (at least one proposal must match the settings on the Cisco router)
<b>Local Port</b>	0
<b>Remote Port</b>	0
<b>Protocol</b>	47

4. Click *OK*.
5. If the Cisco router is configured to use transport mode IPsec, configure transport mode on the FortiGate:

```
config vpn phase2-interface
 edit tocisco_p2
 set encapsulation transport-mode
```



```
 next
end
```

**To configure route-based IPsec in the CLI:**

```
config vpn ipsec phase1-interface
 edit tocisco
 set interface port1
 set proposal 3des-sha1 aes128-sha1
 set remote-gw 192.168.5.113
 set psksecret xxxxxxxxxxxxxxxxx
 next
end

config vpn ipsec phase2-interface
 edit tocisco_p2
 set phase1name tocisco
 set proposal 3des-md5
 set encapsulation [tunnel-mode | transport-mode]
 set protocol 47
 set src-addr-type ip
 set dst-start-ip 192.168.5.113
 set src-start-ip 172.20.120.141
 next
end
```

**To add the IPsec tunnel end addresses:**

```
config system interface
 edit tocisco
 set ip 172.20.120.141 255.255.255.255
 set remote-ip 192.168.5.113
 next
end
```

**Configuring the GRE tunnel**

The local gateway and remote gateway addresses must match the local and remote gateways of the IPsec tunnel. The GRE tunnel runs between the virtual IPsec public interface on the FortiGate unit and the Cisco router.

**To configure the GRE tunnel:**

```
config system gre-tunnel
 edit gre1
 set interface tocisco
 set local-gw 172.20.120.141
 set remote-gw 192.168.5.113
 set keepalive-interval <integer>
 set keepalive-failtimes <integer>
 next
end
```

The Cisco router configuration requires an address for its end of the GRE tunnel, so you need to add the tunnel end addresses.

**To add the tunnel end addresses:**

```
config system interface
 edit gre1
 set ip 10.0.1.1 255.255.255.255
 set remote-ip 10.0.1.2
 next
end
```

**Configuring the security policies**

Two sets of security policies are required:

- Policies to allow traffic to pass in both directions between the GRE virtual interface and the IPsec virtual interface.
- Policies to allow traffic to pass in both directions between the protected network interface and the GRE virtual interface.

**To configure security policies in the GUI:**

1. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
2. Enter the following to allow traffic between the protected network and the GRE tunnel:

<b>Name</b>	LANtoGRE
<b>Incoming Interface</b>	Interface that connects to the private network behind the FortiGate (port2)
<b>Outgoing Interface</b>	GRE tunnel virtual interface (gre1)
<b>Source</b>	All
<b>Destination</b>	All
<b>Action</b>	ACCEPT
<b>NAT</b>	Disable

3. Click *OK*.
4. Create a new policy and enter the following to allow traffic between the GRE tunnel and the protected network:

<b>Name</b>	GREtoLAN
<b>Incoming Interface</b>	GRE tunnel virtual interface (gre1)
<b>Outgoing Interface</b>	Interface that connects to the private network behind the FortiGate (port2)
<b>Source</b>	All
<b>Destination</b>	All
<b>Action</b>	ACCEPT
<b>NAT</b>	Disable

5. Click *OK*.
6. Create a new policy and enter the following to allow traffic between the GRE virtual interface and the IPsec virtual interface:

<b>Name</b>	GREtoIPsec
<b>Incoming Interface</b>	GRE tunnel virtual interface (gre1)
<b>Outgoing Interface</b>	Virtual IPsec interface (tocisco)
<b>Source</b>	All
<b>Destination</b>	All
<b>Action</b>	ACCEPT
<b>NAT</b>	Disable

7. Click *OK*.
8. Create a new policy and enter the following to allow traffic between the IPsec virtual interface and the GRE virtual interface:

<b>Name</b>	IPsectoGRE
<b>Incoming Interface</b>	Virtual IPsec interface (tocisco)
<b>Outgoing Interface</b>	GRE tunnel virtual interface (gre1)
<b>Source</b>	All
<b>Destination</b>	All
<b>Action</b>	ACCEPT
<b>NAT</b>	Disable

9. Click *OK*.

### To configure security policies in the CLI:

```
config firewall policy
edit 1
 set name LANtoGRE
 set srcintf port2
 set dstintf gre1
 set srcaddr all
 set dstaddr all
 set action accept
 set schedule always
 set service ALL
next
edit 2
 set name GREtoLAN
 set srcintf gre1
 set dstintf port2
 set srcaddr all
 set dstaddr all
 set action accept
 set schedule always
 set service ALL
next
edit 3
 set name GREtoIPsec
```

```

 set srcintf gre1
 set dstintf tocisco
 set srcaddr all
 set dstaddr all
 set action accept
 set schedule always
 set service ALL
 next
 edit 4
 set name IPsectoGRE
 set srcintf tocisco
 set dstintf gre1
 set srcaddr all
 set dstaddr all
 set action accept
 set schedule always
 set service ALL
 next
end

```

## Configuring routing

to direct traffic destined for the network behind the Cisco router into the GRE-over-IPsec tunnel Traffic destined for the network behind the Cisco router must be routed to the GRE tunnel. To do this, create a static route

### To create the static route in the GUI:

1. Go to *Network > Static Routes* and click *Create New*.
2. Enter the following:

<b>Destination</b>	IP and netmask for the network behind the Cisco router (10.21.101.0 255.255.255.0)
<b>Interface</b>	GRE tunnel virtual interface (gre1)
<b>Administrative Distance</b>	Leave the default setting

3. Click *OK*.

### To create the static route in the CLI:

```

config router static
 edit 0
 set device gre1
 set dst 10.21.101.0 255.255.255.0
 next
end

```

## Configuring the Cisco router

For more information, refer to [Configuring and verifying a GRE over IPsec tunnel](#) in the Fortinet Knowledge Base.

## Remote access

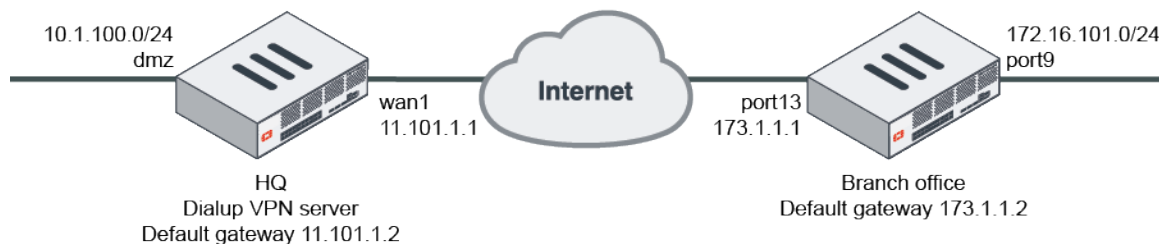
Remote access lets users connect to the Internet using a dialup connection over traditional POTS or ISDN telephone lines. Virtual private network (VPN) protocols are used to secure these private connections.

The following topics provide instructions on configuring remote access:

- [FortiGate as dialup client on page 1199](#)
- [FortiClient as dialup client on page 1205](#)
- [Add FortiToken multi-factor authentication on page 1210](#)
- [Add LDAP user authentication on page 1211](#)
- [iOS device as dialup client on page 1212](#)
- [IKE Mode Config clients on page 1216](#)
- [IPsec VPN with external DHCP service on page 1220](#)
- [L2TP over IPsec on page 1226](#)
- [Tunneled Internet browsing on page 1231](#)
- [Dialup IPsec VPN with certificate authentication on page 1236](#)
- [Restricting VPN access to rogue/non-compliant devices with Security Fabric](#)

### FortiGate as dialup client

This is a sample configuration of dialup IPsec VPN and the dialup client. In this example, a branch office FortiGate connects via dialup IPsec VPN to the HQ FortiGate.



You can configure dialup IPsec VPN with FortiGate as the dialup client using the [GUI](#) or [CLI](#).

#### To configure IPsec VPN with FortiGate as the dialup client in the GUI:

1. Configure the dialup VPN server FortiGate:
  - a. Go to *VPN > IPsec Wizard* and configure the following settings for *VPN Setup*:
    - i. Enter a VPN name.
    - ii. For *Template Type*, select *Site to Site*.
    - iii. For *Remote Device Type*, select *FortiGate*.
    - iv. For *NAT Configuration*, select *The remote site is behind NAT*.
    - v. Click *Next*.
  - b. Configure the following settings for *Authentication*:
    - i. For *Incoming Interface*, select the incoming interface.
    - ii. For *Authentication Method*, select *Pre-shared Key*.
    - iii. In the *Pre-shared Key* field, enter *your-psk* as the key.
    - iv. Click *Next*.

- c. Configure the following settings for *Policy & Routing*:
  - i. From the *Local Interface* dropdown menu, select the local interface.
  - ii. Configure the *Local Subnets* as *10.1.100.0/24*.
  - iii. Configure the *Remote Subnets* as *172.16.101.0/24*.
  - iv. Click *Create*.
2. Configure the dialup VPN client FortiGate:
  - a. Go to *VPN > IPsec Wizard* and configure the following settings for *VPN Setup*:
    - i. Enter a VPN name.
    - ii. For *Template Type*, select *Site to Site*.
    - iii. For *Remote Device Type*, select *FortiGate*.
    - iv. For *NAT Configuration*, select *This site is behind NAT*.
    - v. Click *Next*.
  - b. Configure the following settings for *Authentication*:
    - i. For *IP Address*, enter *11.101.1.1*.
    - ii. For *Outgoing Interface*, select *port13*.
    - iii. For *Authentication Method*, select *Pre-shared Key*.
    - iv. In the *Pre-shared Key* field, enter *your-psk* as the key.
    - v. Click *Next*.
  - c. Configure the following settings for *Policy & Routing*:
    - i. From the *Local Interface* dropdown menu, select the local interface. In this example, it is *port9*.
    - ii. Configure the *Local Subnets* as *172.16.101.0*.
    - iii. Configure the *Remote Subnets* as *10.1.100.0*.
    - iv. Click *Create*.

### To configure IPsec VPN with FortiGate as the dialup client in the CLI:

1. In the CLI, configure the user, user group, and firewall address. Only the HQ dialup server FortiGate needs this configuration. The address is an IP pool to assign an IP address for the dialup client FortiGate.

```
config user local
 edit "vpnuser1"
 set type password
 set passwd your-password
 next
end
config user group
 edit "vpngroup"
 set member "vpnuser1"
 next
end
config firewall address
 edit "client_range"
 set type iprange
 set start-ip 10.10.10.1
 set end-ip 10.10.10.200
 next
end
```

2. Configure the WAN interface and default route. The WAN interface is the interface connected to the ISP. It can work in static mode (as shown in this example), DHCP, or PPPoE mode. The IPsec tunnel is established over the WAN interface.

**a. Configure the HQ FortiGate.**

```
config system interface
 edit "wan1"
 set vdom "root"
 set ip 11.101.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 11.101.1.2
 set device "wan1"
 next
end
```

**b. Configure the branch office FortiGate.**

```
config system interface
 edit "port13"
 set vdom "root"
 set ip 173.1.1.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 173.1.1.2
 set device "port13"
 next
end
```

**3. Configure the internal interface and protected subnet. The internal interface connects to the internal network. Traffic from this interface will route out the IPsec VPN tunnel.****a. Configure the HQ FortiGate.**

```
config system interface
 edit "dmz"
 set vdom "root"
 set ip 10.1.100.1 255.255.255.0
 next
end
config firewall address
 edit "10.1.100.0"
 set subnet 10.1.100.0 255.255.255.0
 next
end
```

**b. Configure the branch office FortiGate.**

```
config system interface
 edit "port9"
 set vdom "root"
 set ip 172.16.101.1 255.255.255.0
 next
end
config firewall address
 edit "172.16.101.0"
 set subnet 172.16.101.0 255.255.255.0
 next
end
```

- 4. Configure the IPsec phase1-interface. In this example, PSK is used as the authentication method. Signature authentication is also an option.**

**a. Configure the HQ FortiGate.**

```
config vpn ipsec phase1-interface
 edit "for_Branch"
 set type dynamic
 set interface "wan1"
 set mode aggressive
 set peertype any
 set mode-cfg enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set add-route disable
 set dpd on-idle
 set xauthtype auto
 set authusrgrp "vpngroup"
 set net-device enable
 set assign-ip-from name
 set dns-mode auto
 set ipv4-split-include "10.1.100.0"
 set ipv4-name "client_range"
 set save-password enable
 set psksecret sample
 set dpd-retryinterval 60
 next
end
```

**b. Configure the branch office FortiGate.**

```
config vpn ipsec phase1-interface
 edit "to_HQ"
 set interface "port13"
 set mode aggressive
 set peertype any
 set mode-cfg enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set add-route disable
 set xauthtype client
 set authusr "vpnuser1"
 set authpasswd vpnuser1-password
 set remote-gw 11.101.1.1
 set psksecret sample
 next
end
```

- 5. Configure the IPsec phase2-interface.**

**a. Configure the HQ FortiGate:**

```
config vpn ipsec phase2-interface
 edit "for_Branch_p2"
 set phase1 name "for_Branch"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 next
end
```



**b. Configure the branch office FortiGate.**

```
config vpn ipsec phase2-interface
 edit "to_HQ_p2"
 set phase1name "to_HQ"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 next
end
```

**6. Configure the static routes on the branch office FortiGate. The blackhole route is important to ensure that IPsec traffic does not match the default route when the IPsec tunnel is down.**

```
config router static
 edit 2
 set dst 10.1.100.0 255.255.255.0
 set device "to_HQ"
 next
 edit 3
 set dst 10.1.100.0 255.255.255.0
 set blackhole enable
 set distance 254
 next
end
```

**7. Configure the firewall policy to allow the branch office to HQ network flow over the IPsec tunnel. This configuration only supports traffic from the branch office FortiGate to the HQ FortiGate. Traffic is dropped from the HQ FortiGate to the branch office FortiGate.****a. Configure the HQ FortiGate.**

```
config firewall policy
 edit 1
 set name "inbound"
 set srcintf "for_Branch"
 set dstintf "dmz"
 set srcaddr "172.16.101.0"
 set dstaddr "10.1.100.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end
```

**b. Configure the branch office FortiGate.**

```
config firewall policy
 edit 1
 set name "outbound"
 set srcintf "port9"
 set dstintf "to_HQ"
 set srcaddr "172.16.101.0"
 set dstaddr "10.1.100.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end
```

8. Run diagnose commands to check the IPsec phase1/phase2 interface status. The diagnose debug application ike -l command is the key to troubleshoot why the IPsec tunnel failed to establish.
- a. Run the diagnose vpn ike gateway list command on the HQ FortiGate. The system should return the following:

```
vd: root/0
name: for_Branch_0
version: 1
interface: wan1 5
addr: 11.101.1.1:500 -> 173.1.1.1:500
created: 1972s ago
xauth-user: vpnuser1
assigned IPv4 address: 10.10.10.1/255.255.255.252
IKE SA: created 1/1 established 1/1 time 10/10/10 ms
IPsec SA: created 1/1 established 1/1 time 0/0/0 ms
id/spi: 184 5b1c59fab2029e43/bf517e686d3943d2
direction: responder
status: established 1972-1972s ago = 10ms
proposal: aes128-sha256
key: 8046488e92499247-fbbb4f6dfa4952d0
lifetime/rekey: 86400/84157
DPD sent/recvd: 00000020/00000000
```

- b. Run the diagnose vpn tunnel list command on the HQ FortiGate. The system should return the following:

```
list all ipsec tunnel in vd 0
name=for_Branch_0 ver=1 serial=9 11.101.1.1:0->173.1.1.1:0
bound_if=5 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/208 options
[00d0]=create_dev no-sysctlrgwy-chg
parent=for_Branch index=0
proxyid_num=1 child_num=0 refcnt=12 ilast=8 olast=8 ad=/0
stat: rxp=8 txp=8 rxb=1216 txb=672
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=31
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=for_Branch_p2 proto=0 sa=1 ref=2 serial=1
src: 0:0.0.0.0-255.255.255.255:0
dst: 0:0.0.0.0-255.255.255.255:0
SA: ref=3 options=226 type=00 soft=0 mtu=1438 expire=41297/0B replaywin=2048 seqno=9
esn=0 replaywin_lastseq=00000009 itn=0
life: type=01 bytes=0/0 timeout=43190/43200
dec: spi=747c10c6 esp=aes key=16 278c2430e09e74f1e229108f906603b0
ah=sha1 key=20 21dad76b008d1e8b8e53148a2fcbd013a277974a
enc: spi=ca646448 esp=aes key=16 b7801d125804e3610a556da7caefd765
ah=sha1 key=20 a70164c3094327058bd84c1a0c954ca439709206
dec:pkts/bytes=8/672, enc:pkts/bytes=8/1216

name=for_Branchver=1 serial=6 11.101.1.1:0->0.0.0.0:0
bound_if=5 lgwy=static/1 tun=intf/0 mode=dialup/2 encap=none/16 options[0010]=create_dev
proxyid_num=0 child_num=1 refcnt=14 ilast=8523 olast=8523 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=0
```

- c. Run the diagnose vpn ike gateway list command on the branch office FortiGate. The system should return the following:

```

vd: root/0
name: to_HQ
version: 1
interface: port13 42
addr: 173.1.1.1:500 -> 11.101.1.1:500
created: 2016s ago
assigned IPv4 address: 10.10.10.1/255.255.255.252
IKE SA: created 1/1 established 1/1 time 0/0/0 ms
IPsec SA: created 1/1 established 1/1 time 0/0/0 ms
id/spi: 93 5blc59fab2029e43/bf517e686d3943d2
direction: initiator
status: established 2016-2016s ago = 0ms
proposal: aes128-sha256
key: 8046488e92499247-fbbb4f6dfa4952d0
lifetime/rekey: 86400/84083
DPD sent/recvd: 00000000/00000020

```

- d. Run the `diagnose vpn tunnel list` command on the branch office FortiGate. The system should return the following:

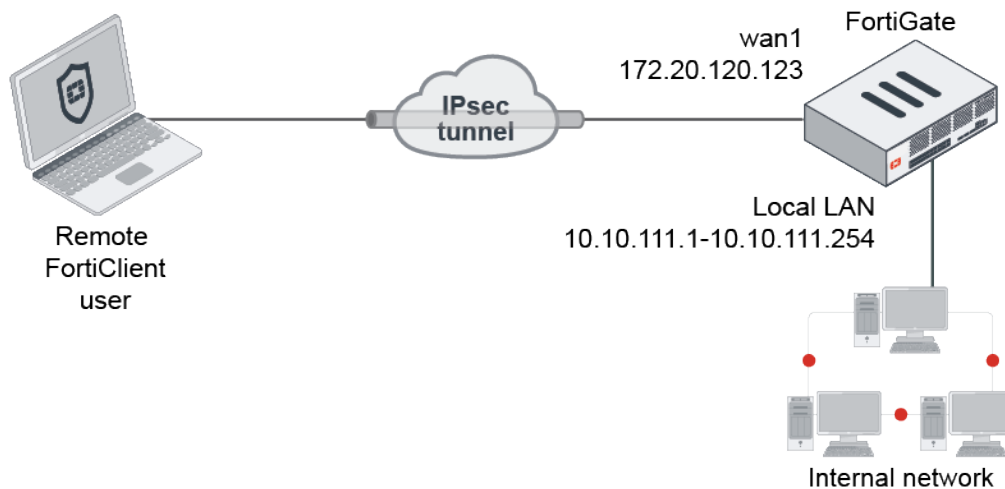
```

list all ipsec tunnel in vd 0
name=to_HQver=1 serial=7 173.1.1.1:0->11.101.1.1:0
bound_if=42 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/8 options[0008]=npu
proxyid_num=1 child_num=0 refcnt=13 ilast=18 olast=58 ad=/0
stat: rxp=1 txp=2 rxb=152 txb=168
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=to_HQ proto=0 sa=1 ref=2 serial=1
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=6 options=10226 type=00 soft=0 mtu=1438 expire=41015/0B replaywin=2048
seqno=3 esn=0 replaywin_lastseq=00000002 itn=0
life: type=01 bytes=0/0 timeout=42898/43200
dec: spi=ca646448 esp=aes key=16 b7801d125804e3610a556da7caefd765
ah=sha1 key=20 a70164c3094327058bd84c1a0c954ca439709206
enc: spi=747c10c6 esp=aes key=16 278c2430e09e74f1e229108f906603b0
ah=sha1 key=20 21dad76b008d1e8b8e53148a2fcbd013a277974a
dec:pkts/bytes=1/84, enc:pkts/bytes=2/304
npu_flag=03 npu_rgwy=11.101.1.1 npu_lgwy=173.1.1.1 npu_selid=5 dec_npuid=2 enc_
npuid=2

```

## FortiClient as dialup client

This is a sample configuration of dialup IPsec VPN with FortiClient as the dialup client.



You can configure dialup IPsec VPN with FortiClient as the dialup client using the GUI or CLI.

If multiple dialup IPsec VPNs are defined for the same dialup server interface, each phase1 configuration must define a unique peer ID to distinguish the tunnel that the remote client is connecting to. When a client connects, the first IKE message that is in aggressive mode contains the client's local ID. FortiGate matches the local ID to the dialup tunnel referencing the same Peer ID, and the connection continues with that tunnel.

### To configure IPsec VPN with FortiClient as the dialup client on the GUI:

1. Configure a user and user group.
  - a. Go to *User & Device > User Definition* to create a local user *vpnuser1*.
  - b. Go to *User & Device > User Groups* to create a group *vpngroup* with the member *vpnuser1*.
2. Go to *VPN > IPsec Wizard* and configure the following settings for *VPN Setup*:
  - a. Enter a VPN name.
  - b. For *Template Type*, select *Remote Access*.
  - c. For *Remote Device Type*, select *Client-based > FortiClient*.
  - d. Click *Next*.
3. Configure the following settings for *Authentication*:
  - a. For *Incoming Interface*, select *wan1*.
  - b. For *Authentication Method*, select *Pre-shared Key*.
  - c. In the *Pre-shared Key* field, enter *your-psk* as the key.
  - d. From the *User Group* dropdown list, select *vpngroup*.
  - e. Click *Next*.
4. Configure the following settings for *Policy & Routing*:
  - a. From the *Local Interface* dropdown menu, select *lan*.
  - b. Configure the *Local Address* as *local\_network*.
  - c. Configure the *Client Address Range* as *10.10.2.1-10.10.2.200*.
  - d. Keep the default values for the *Subnet Mask*, *DNS Server*, *Enable IPv4 Split tunnel*, and *Allow Endpoint Registration*.
  - e. Click *Next*.
5. Adjust the *Client Options* as needed, then click *Create*.

6. Optionally, define a unique Peer ID in the phase1 configuration:
  - a. Go to *VPN > IPsec Tunnels* and edit the just created tunnel.
  - b. Click *Convert To Custom Tunnel*.
  - c. In the *Authentication* section, click *Edit*.
  - d. Under *Peer Options*, set *Accept Types* to *Specific peer ID*.
  - e. In the *Peer ID* field, enter a unique ID, such as *dialup1*.
  - f. Click *OK*.

### To configure IPsec VPN with FortiClient as the dialup client using the CLI:

1. In the CLI, configure the user and group.

```
config user local
 edit "vpnuser1"
 set type password
 set passwd your-password
 next
end
config user group
 edit "vpngroup"
 set member "vpnuser1"
 next
end
```

2. Configure the internal interface. The LAN interface connects to the corporate internal network. Traffic from this interface routes out the IPsec VPN tunnel. Creating an address group for the protected network behind this FortiGate causes traffic to this network group to go through the IPsec tunnel.

```
config system interface
 edit "lan"
 set vdom "root"
 set ip 10.10.111.1 255.255.255.0
 next
end
config firewall address
 edit "local_subnet_1"
 set subnet 10.10.111.0 255.255.255.0
 next
 edit "local_subnet_2"
 set subnet 10.10.112.0 255.255.255.0
 next
end
config firewall addrgrp
 edit "local_network"
 set member "local_subnet_1" "local_subnet_2"
 next
end
```

3. Configure the WAN interface. The WAN interface is the interface connected to the ISP. It can work in static mode (as shown in this example), DHCP, or PPPoE mode. The IPsec tunnel is established over the WAN interface.

```
config system interface
 edit "wan1"
 set vdom "root"
 set ip 172.20.120.123 255.255.255.0
```

```
 next
end
```

4. Configure the client address pool. You must create a firewall address to assign an IP address to a client from the address pool.

```
config firewall address
 edit "client_range"
 set type iprange
 set comment "VPN client range"
 set start-ip 10.10.2.1
 set end-ip 10.10.2.200
 next
end
```

5. Configure the IPsec phase1-interface. In this example, PSK is used as the authentication method. Signature authentication is also an option.

```
config vpn ipsec phase1-interface
 edit "for_client"
 set type dynamic
 set interface "wan1"
 set mode aggressive
 set peertype one
 set peerid "dialup1"
 set net-device enable
 set mode-cfg enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set dpd on-idle
 set xauthtype auto
 set authusrgrp "vpngroup"
 set assign-ip-from name
 set ipv4-name "client_range"
 set dns-mode auto
 set ipv4-split-include "local_network"
 set save-password enable
 set psksecret your-psk
 set dpd-retryinterval 60
 next
end
```

6. Configure the IPsec phase2-interface.

```
config vpn ipsec phase2-interface
 edit "for_client"
 set phase1name "for_client"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 next
end
```

7. Configure the firewall policy to allow client traffic flow over the IPsec VPN tunnel.

```
config firewall policy
 edit 1
 set name "inbound"
 set srcintf "for_client"
 set dstintf "lan"
 set srcaddr "client_range"
```

```

 set dstaddr "local_network"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end

```

### To configure FortiClient:

1. In FortiClient, go to *Remote Access* and click *Add a new connection*.
2. Set the *VPN* to *IPsec VPN* and the *Remote Gateway* to the FortiGate IP address.
3. Set the *Authentication Method* to *Pre-Shared Key* and enter the key.
4. Expand *Advanced Settings > Phase 1* and in the *Local ID* field, enter *dialup1*.
5. Configure remaining settings as needed, then click *Save*.
6. Select the VPN, enter the username and password, then select *Connect*.

### Diagnose the connection

Run `diagnose` commands to check the IPsec phase1/phase2 interface status. The `diagnose debug application ike -1` command is the key to troubleshoot why the IPsec tunnel failed to establish.

1. Run the `diagnose vpn ike gateway list` command. The system should return the following:

```

vd: root/0
name: for_client_0
version: 1
interface: port1 15
addr: 172.20.120.123:4500 ->172.20.120.254:64916
created: 37s ago
xauth-user: vpnuser1
assigned IPv4 address: 10.10.1.1/255.255.255.255
nat: me peer
IKE SA: created 1/1 established 1/1 time 10/10/10 ms
IPsec SA: created 1/1 established 1/1 time 0/0/0 ms
id/spi: 1 b40a32d878d5e262/8bba553563a498f4
direction: responder
status: established 37-37s ago = 10ms
proposal: aes256-sha256
key: f4ad7ec3a4fcfd09-787e2e9b7bceb9a7-0dfa183240d838ba-41539863e5378381
lifetime/rekey: 86400/86092
DPD sent/recvd: 00000000/00000a0e

```

2. Run the `diagnose vpn tunnel list` command. The system should return the following:

```

list all ipsec tunnel in vd 0
=
=
name=for_client_0 ver=1 serial=3 172.20.120.123:4500->172.20.120.254:64916
bound_if=15 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/984 options
[03d8]=npucrate_dev no-sysctlrgwy-chgrport-chg frag-rfcaccept_traffic=1
parent=for_client index=0
proxyid_num=1 child_num=0 refcnt=12 ilast=3 olast=3 ad=/0
stat: rxp=1 txp=0 rxb=16402 txb=0
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=keepalive draft=32 interval=10 remote_port=64916

```

```

proxyid=for_client proto=0 sa=1 ref=2 serial=1 add-route
src: 0:0.0.0.0-255.255.255.255:0
dst: 0:10.10.1.1-10.10.1.1:0
SA: ref=4 options=2a6 type=00 soft=0 mtu=1422 expire=42867/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000001 itn=0
life: type=01 bytes=0/0 timeout=43189/43200
dec: spi=36274d14 esp=aes key=16 e518b84b3c3b667b79f2e61c64a225a6
ah=sha1 key=20 9ccea544ed042fda800c4fe5d3fd9d8b811984a
enc: spi=8b154deb esp=aes key=16 9d50f004b45c122e4e9fb7af085c457c
ah=sha1 key=20 fld90b2a311049e23be34967008239637b50a328
dec:pkts/bytes=1/16330, enc:pkts/bytes=0/0
npu_flag=02 npu_rgwy=172.20.120.254 npu_lgwy=172.20.120.123npu_selid=0 dec_npuid=2 enc_
npuid=0
name=for_clientver=1 serial=2 172.20.120.123:0->0.0.0.0:0
bound_if=15 lgwy=static/1 tun=intf/0 mode=dialup/2 encap=none/536 options
[0218]=npucrate_dev frag-rfcaccept_traffic=1
proxyid_num=0 child_num=1 refcnt=11 ilast=350 olast=350 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0

```

## Add FortiToken multi-factor authentication

This configuration adds multi-factor authentication (MFA) to the FortiClient dialup VPN configuration ([FortiClient as dialup client on page 1205](#)). It uses one of the two free mobile FortiTokens that is already installed on the FortiGate.

### To configure MFA using the GUI:

1. Edit the user:
  - a. Go to *User & Device > User Definition* and edit local user *vpnuser1*.
  - b. Enter the user's *Email Address*.
  - c. Enable *Two-factor Authentication* and select one mobile *Token* from the list,
  - d. Enable *Send Activation Code* and select *Email*.
  - e. Click *Next* and click *Submit*.
2. Activate the mobile token.
  - a. When a FortiToken is added to user *vpnuser1*, an email is sent to the user's email address. Follow the instructions to install your FortiToken mobile application on your device and activate your token.

### To configure MFA using the CLI:

1. Edit the user and user group:

```

config user local
 edit "vpnuser1"
 set type password
 set two-factor fortitoken
 set fortitoken <select mobile token for the option list>
 set email-to <user's email address>
 set passwd <user's password>
 next
end

```



2. Activate the mobile token.
  - a. When a FortiToken is added to user *vpnuser1*, an email is sent to the user's email address. Follow the instructions to install your FortiToken mobile application on your device and activate your token.

## Add LDAP user authentication

This configuration adds LDAP user authentication to the FortiClient dialup VPN configuration ([FortiClient as dialup client on page 1205](#)). You must have already generated and exported a CA certificate from your AD server.

### To configure LDAP user authentication using the GUI:

1. Import the CA certificate into FortiGate:
  - a. Go to *System > Certificates*.  
If the *Certificates* option is not visible, enable it in *Feature Visibility*. See [Feature visibility on page 732](#) for details.
  - b. Click *Import > CA Certificate*.
  - c. Set *Type* to *File*.
  - d. Click *Upload* then find and select the certificate file.
  - e. Click *OK*.  
The CA certificate now appears in the list of *External CA Certificates*. In this example, it is called *CA\_Cert\_1*.
  - f. Optionally, rename the system generated *CA\_Cert\_1* to something more descriptive:

```
config vpn certificate ca
 rename CA_Cert_1 to LDAPS-CA
end
```

2. Configure the LDAP user:
  - a. Go to *User & Device > LDAP Servers* and click *Create New*.
  - b. Set *Name* to *ldaps-server* and specify *Server IP/Name*.
  - c. Specify *Common Name Identifier* and *Distinguished Name*.
  - d. Set *Bind Type* to *Regular*.
  - e. Specify *Username* and *Password*.
  - f. Enable *Secure Connection* and set *Protocol* to *LDAPS*.
  - g. For *Certificate*, select *LDAP server CA LDAPS-CA* from the list.
  - h. Click *OK*.
3. Add the LDAP user to the user group:
  - a. Go to *User & Device > User Groups* and edit the *vpngroup* group.
  - b. In *Remote Groups*, click *Add* to add the *ldaps-server* remote server.
  - c. Click *OK*.

### To configure LDAP user authentication using the CLI:

1. Import the CA certificate using the GUI.
2. Configure the LDAP user:

```
config user ldap
 edit "ldaps-server"
 set server "172.20.120.161"
 set cnid "cn"
```

```

 set dn "cn=Users,dc=qa,dc=fortinet,dc=com"
 set type regular
 set username "CN=Administrator,cn=users,DC=qa,DC=fortinet,DC=com"
 set password *****
 set group-member-check group-object
 set secure ldaps
 set ca-cert "LDAPS-CA"
 set port 636
 next
end

```

### 3. Add the LDAP user to the user group:

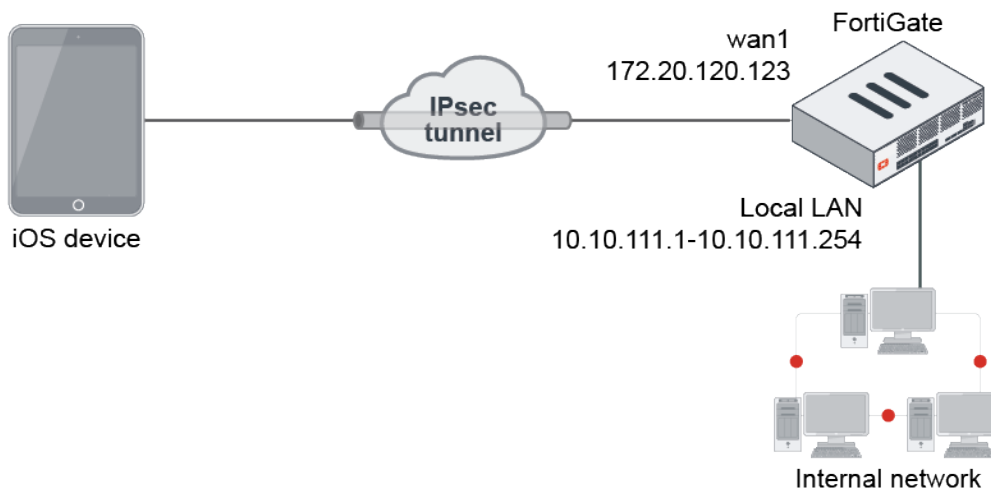
```

config user group
 edit "vpngroup"
 append member "ldaps-server"
 next
end

```

## iOS device as dialup client

This is a sample configuration of dialup IPsec VPN with an iPhone or iPad as the dialup client.



You can configure dialup IPsec VPN with an iOS device as the dialup client using the [GUI](#) or [CLI](#).

### To configure IPsec VPN with an iOS device as the dialup client on the GUI:

1. Go to *VPN > IPsec Wizard* and configure the following settings for *VPN Setup*:
  - a. Enter a VPN name.
  - b. For *Template Type*, select *Remote Access*.
  - c. For *Remote Device Type*, select *Native > iOS Native*.
  - d. For *NAT Configuration*, set *No NAT Between Sites*.
  - e. Click *Next*.
2. Configure the following settings for *Authentication*:
  - a. For *Incoming Interface*, select *wan1*.
  - b. For *Authentication Method*, select *Pre-shared Key*.

- c. In the *Pre-shared Key* field, enter *your-psk* as the key.
  - d. From the *User Group* dropdown list, select *vpngroup*.
  - e. Deselect *Require 'Group Name' on VPN client*.
  - f. Click *Next*.
3. Configure the following settings for *Policy & Routing*:
  - a. From the *Local Interface* dropdown menu, select *lan*.
  - b. Configure the *Local Address* as *local\_network*.
  - c. Configure the *Client Address Range* as *10.10.2.1-10.10.2.200*.
  - d. Keep the default values for the *Subnet Mask*, *DNS Server*, and *Enable IPv4 Split tunnel*.
  - e. Click *Create*.

**To configure IPsec VPN with an iOS device as the dialup client using the CLI:**

1. In the CLI, configure the user and group.

```
config user local
 edit "vpnuser1"
 set type password
 set passwd your-password
 next
end
config user group
 edit "vpngroup"
 set member "vpnuser1"
 next
end
```

2. Configure the internal interface. The LAN interface connects to the corporate internal network. Traffic from this interface routes out the IPsec VPN tunnel. Creating an address group for the protected network behind this FortiGate causes traffic to this network group to go through the IPsec tunnel.

```
config system interface
 edit "lan"
 set vdom "root"
 set ip 10.10.111.1 255.255.255.0
 next
end
config firewall address
 edit "local_subnet_1"
 set subnet 10.10.111.0 255.255.255.0
 next
 edit "local_subnet_2"
 set subnet 10.10.112.0 255.255.255.0
 next
end
config firewall addrgrp
 edit "local_network"
 set member "local_subnet_1" "local_subnet_2"
 next
end
```

3. Configure the WAN interface. The WAN interface is the interface connected to the ISP. It can work in static mode (as shown in this example), DHCP, or PPPoE mode. The IPsec tunnel is established over the WAN interface.

```
config system interface
 edit "wan1"
 set vdom "root"
 set ip 172.20.120.123 255.255.255.0
 next
end
```

4. Configure the client address pool. You must create a firewall address to assign an IP address to a client from the address pool.

```
config firewall address
 edit "client_range"
 set type iprange
 set comment "VPN client range"
 set start-ip 10.10.2.1
 set end-ip 10.10.2.200
 next
end
```

5. Configure the IPsec phase1-interface. In this example, PSK is used as the authentication method. Signature authentication is also an option.

```
config vpn ipsec phase1-interface
 edit "for_ios_p1"
 set type dynamic
 set interface "wan1"
 set peertype any
 set net-device enable
 set mode-cfg enable
 set proposal aes256-sha256 aes256-md5 aes256-sha1
 set dpd on-idle
 set dhgrp 14 5 2
 set xauthtype auto
 set authusrgrp "vpngroup"
 set assign-ip-from name
 set ipv4-name "client_range"
 set dns-mode auto
 set ipv4-split-include "local_network"
 set psksecret your-psk
 set dpd-retryinterval 60
 next
end
```

6. Configure the IPsec phase2-interface.

```
config vpn ipsec phase2-interface
 edit "for_ios_p2"
 set phaselname "for_ios_p1"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 set pfs disable
 set keepalive enable
 next
end
```

7. Configure the firewall policy to allow client traffic flow over the IPsec VPN tunnel.

```
config firewall policy
 edit 1
```

```

 set name "ios_vpn"
 set srcintf "for_ios_p1"
 set dstintf "lan"
 set srcaddr "ios_range"
 set dstaddr "local_network"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end

```

## 8. Configure the iOS device.

- a. In the iOS device, go to **Settings > General > VPN** and select **Add VPN Configuration**.
- b. Set the **Type** to **IPsec** and enter a **Description**. Set the **Server** to the FortiGate's Internet-facing interface, and enter the username in **Account**. Enter the user password, the preshared IPsec VPN secret, then select **Done**.
- c. Ensure that the IPsec VPN configuration is highlighted (indicated by a checkmark), and select the **Not Connected** button. The IPsec VPN connects with the user's credentials and secret. The status changes to **Connected**, and a VPN icon appears at the top of the screen.

## 9. Run diagnose commands to check the IPsec phase1/phase2 interface status. The `diagnose debug application ike -1` command is the key to troubleshoot why the IPsec tunnel failed to establish.

- a. Run the `diagnose vpn ike gateway list` command. The system should return the following:

```

vd: root/0
name: for_ios_p1_0
version: 1
interface: port1 15
addr: 172.20.120.123:4500 -> 172.20.120.254:64916
created: 17s ago
xauth-user: ul
assigned IPv4 address: 10.10.2.1/255.255.255.255
nat: me peer
IKE SA: created 1/1 established 1/1 time 150/150/150 ms
IPsec SA: created 1/1 established 1/1 time 10/10/10 ms
id/spi: 2 3c844e13c75591bf/80c2db92c8d3f602 direction: responder status: established
17-17s ago = 150ms proposal: aes256-sha256 key: 0032ea5ee160d775-51f3bf1f9909101b-
b89c7b5a77a07784-2c92cf9c921801ac lifetime/rekey: 3600/3312 DPD sent/recvd:
00000000/00000000

```

- b. Run the `diagnose vpn tunnel list` command. The system should return the following:

```

list all ipsec tunnel in vd 0
=
=
name=for_ios_p1_0 ver=1 serial=172.20.120.123:4500->172.20.120.254:64916
bound_if=15 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/984 options
[03d8]=npu create_dev no-sysctl rgwy-chg rport-chg frag-rfc accept_traffic=1
parent=for_ios_p1 index=0
proxymid_num=1 child_num=0 refcnt=12 ilast=23 olast=23 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=0
natt: mode=keepalive draft=32 interval=10 remote_port=64916
proxymid=for_ios_p1 proto=0 sa=1 ref=2 serial=1 add-route
src: 0:10.10.111.0-10.10.111.255:0 dst: 0:10.10.2.1-10.10.2.1:0 SA: ref=3 options=a7
type=00 soft=0 mtu=1422 expire=3564/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000000 itn=0
life: type=01 bytes=0/0 timeout=3587/3600 dec: spi=36274d15 esp=aes key=32

```

```

5a599d796f8114c83d6589284f036fc33bdf4456541e2154b4ac2217b6aec869
ah=sha1 key=20 f1efdeb77d6f856a8dd3a30cbc23cb0f8a3e0340
enc: spi=00b0d9ab esp=aes key=32
e9232d7a1c4f390fd09f8409c2d85f80362d940c08c73f245908ab1ac3af322f
ah=sha1 key=20 a3890d6c5320756291cad85026d3a78fd42a1b42
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0 npu_flag=00 npu_rgw=172.20.120.254 npu_
lgwy=172.20.120.123 npu_selid=1 dec_npuid=0 enc_npuid=0

```

## IKE Mode Config clients

IKE Mode Config is an alternative to DHCP over IPsec. It allows dialup VPN clients to obtain virtual IP address, network, and DNS configurations amongst others from the VPN server. A FortiGate can be configured as either an IKE Mode Config server or client.

IKE Mode Config can configure the host IP address, domain, DNS addresses, and WINS addresses. IPsec parameters such as gateway address, encryption, and authentication algorithms must be configured. Several network equipment vendors support IKE Mode Config.

An IKE Mode Config server or client is configured using `config vpn ipsec phase1-interface` and involves the following parameters:

Parameter	Description
ike-version {1   2}	IKE v1 is the default for FortiGate IPsec VPNs. IKE Mode Config is also compatible with IKE v2.
mode-cfg {enable   disable}	Enable/disable IKE Mode Config.
type {static   dynamic   ddns}	If you set <code>type</code> to <code>dynamic</code> , an IKE Mode Config server is created. The other settings create an IKE Mode Config client.
assign-ip {enable   disable}	Enable to request an IP address from the server. This configuration is for IKE Mode Config clients only.
interface <interface_name>	Specify the physical, aggregate, or VLAN interface to which the IPsec tunnel will be bound.
proposal <encryption_ combination>	The encryption and authentication settings that the client will accept.
ip-version {4   6}	By default, IPsec VPNs use IPv4 addressing.
ipv4-split-include <string> ipv6-split-include <string>	Mode Config server configuration. Applicable to IKEv1 and IKEv2. Specify the firewall address or address group that represents the subnets that the clients will have access to. This information is sent to the clients so that default traffic should not flow over the IPsec tunnel except for the specified subnets.
split-include-service <string>	Mode Config server configuration. Applicable to IKEv1 and IKEv2. Specify the service or service group that represents the services that the clients will have access to. This information is sent to the clients so that default traffic should not flow over the IPsec tunnel except for the specified services.
ipv4-split-exclude <string> ipv6-split-exclude <string>	Specify the subnets that should not be accessed over the IPsec tunnel. This information is sent to the clients so that all default traffic should flow over the IPsec tunnel except for the specified subnets.

Parameter	Description
	See <a href="#">Split-exclude in IKEv1</a> .

## Creating an IKE Mode Config client

In this example, the FortiGate connects to a VPN gateway with a static IP address that can be reached through port 1. Only the port, gateway, and proposal information needs to be configured. All other configuration information will come from the IKE Mode Config server.

### To configure an IKE Mode Config client:

```
config vpn ipsec phase1-interface
 edit vpn1
 set ip-version 4
 set type static
 set remote-gw <gw_address>
 set interface port1
 set proposal 3des-sha1 aes128-sha1
 set mode-cfg enable
 set assign-ip enable
 next
end
```

## Split-exclude in IKEv1

The `split-exclude` option specifies that default traffic flows over the IPsec tunnel except for specified subnets. This is the opposite of `split-include`, which specifies that default traffic should not flow over the IPsec tunnel except for specified subnets. The `split-include` and `split-exclude` options can be specified at the same time.

### To configure split-exclude:

```
config vpn ipsec phase1-interface
 edit <name>
 set ike-version 1
 set type dynamic
 set mode-cfg enable
 set ipv4-split-exclude <string>
 set ipv6-split-exclude <string>
 next
end
```

## Creating an IKE Mode Config server

### To configure IKE Mode config settings, the following must be configured first :

```
config vpn ipsec phase1-interface
 edit "vpn-p1"
 set type dynamic
 set interface <interface_name>
 set ike-version < 1 | 2 >
 set mode-cfg enable
```

```
 set proposal <encryption_combination>
 set ip-version < 4 | 6 >
 next
end
```

In this example, the FortiGate assigns IKE Mode Config clients addresses in the range of 10.11.101.160 - 10.11.101.180. DNS and WINS server addresses are also provided. The public interface of the FortiGate unit is port1.

When IKE Mode-Configuration is enabled, multiple server IPs can be defined in IPsec phase 1.

The `ipv4-split-include` parameter specifies a firewall address (`OfficeLAN`), which represents the networks that the clients will have access to. This destination IP address information is sent to the clients.

### To configure an IKE Mode Config server:

```
config vpn ipsec phase1-interface
 edit "vpn-p1"
 set type dynamic
 set interface "wan1"
 set xauthtype auto
 set mode aggressive
 set mode-cfg enable
 set proposal 3des-sha1 aes128-sha1
 set dpd disable
 set dhgrp 2
 set authusrgrp "FG-Group1"
 set ipv4-start-ip 10.10.10.10
 set ipv4-end-ip 10.10.10.20
 set ipv4-dns-server1 1.1.1.1
 set ipv4-dns-server2 2.2.2.2
 set ipv4-dns-server3 3.3.3.3
 set ipv4-wins-server1 4.4.4.4
 set ipv4-wins-server2 5.5.5.5
 set domain "fgt1c-domain"
 set banner "fgt111C-banner"
 set backup-gateway "100.100.100.1" "host1.com" "host2"
 set ipv4-split-include OfficeLAN
 next
end
```

## Assigning IP addresses

Once the basic configuration is enabled, you can configure IP address assignment for clients, as well as DNS and WINS server assignments. Usually you will want to assign IP addresses to clients. The easiest way is to assign addresses from a specific range, similar to a DHCP server.

### To assign an IP from an address range:

```
config vpn ipsec phase1-interface
 edit vpn1
 set ip-version 4
 set assign-ip enable
 set assign-ip-from range
 set ipv4-start-ip <range_start>
 set ipv4-end-ip <range_end>
 set ipv4-netmask <netmask>
```



```
 next
end
```

**To assign an IP from a named firewall address or group:**

```
config vpn ipsec phase1-interface
 edit vpn1
 set type dynamic
 set assign-ip-from name
 set ipv4-name <name>
 set ipv6-name <name>
 next
end
```

**RADIUS server**

If the client is authenticated by a RADIUS server, you can obtain the user's IP address assignment from the Framed-IP-Address attribute. The user must be authenticated using XAuth.

The users must be authenticated by a RADIUS server and assigned to the FortiGate user group <grp\_name>. Since the IP address is not static, type is set to dynamic and `mode-cfg` is enabled. With IKE Mode Config, compatible clients can configure themselves with settings provided by the FortiGate.

**To assign an IP from a RADIUS server:**

```
config vpn ipsec phase1-interface
 edit vpn1
 set type dynamic
 set mode-cfg enable
 set assign-ip enable
 set assign-ip-from usrgroup
 set xauthtype auto
 set authusrgroup <grp_name>
 next
end
```

**DHCP server**

IKE Mode Config can use a remote DHCP server to assign the client IP addresses. Up to eight server addresses can be selected for either IPv4 or IPv6. The DHCP proxy must be enabled first.

**To assign an IP from a DHCP server:**

```
config system settings
 set dhcp-proxy enable
 set dhcp-server-ip <address>
 set dhcp6-server-ip <address>
end

config vpn ipsec phase1-interface
 edit vpn1
 set mode-cfg enable
 set assign-ip-from dhcp
 next
end
```

## Certificate groups

IKE certificate groups consisting of up to four RSA certificates can be used in IKE phase 1. Since CA and local certificates are global, the IKE daemon loads them once for all VDOMs and indexes them into trees based on subject and public key hash (for CA certificates), or certificate name (for local certificates). Certificates are linked together based on the issuer, and certificate chains are built by traversing these links. This reduces the need to keep multiple copies of certificates that could exist in multiple chains.

### To configure the IKE local ID:

```
config vpn certificate local
 edit <name>
 set ike-localid <string>
 set ike-localid-type {asnldn | fqdn}
 next
end
```

## Split-exclude in IKEv1

The `split-exclude` setting specifies that default traffic flows over the IPsec tunnel except for specified subnets. This is the opposite of `split-include`, which specifies that default traffic should not flow over the IPsec tunnel except for specified subnets. The `split-include` and `split-exclude` settings can be specified at the same time.

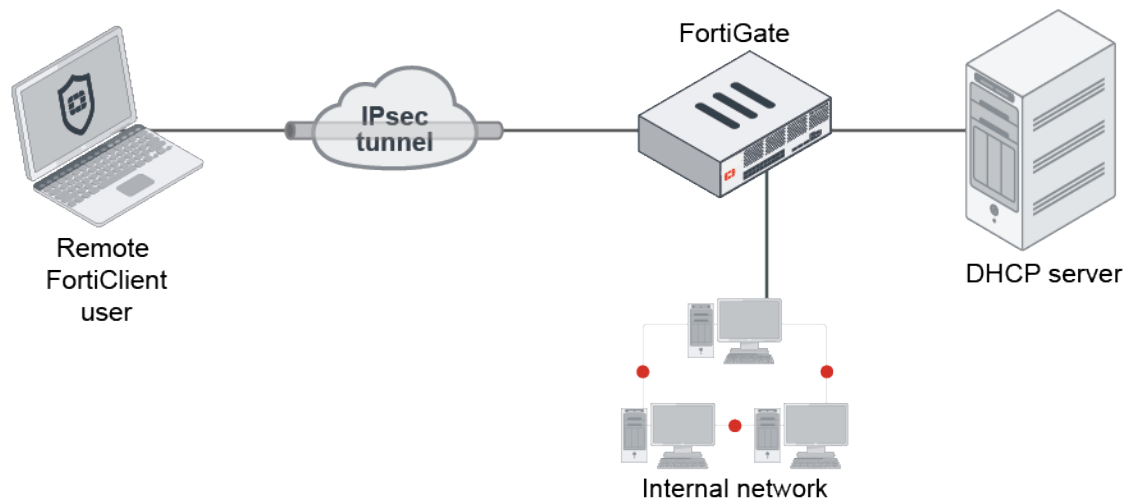
### To configure split-exclude:

```
config vpn ipsec phase1-interface
 edit <name>
 set ike-version 1
 set type dynamic
 set mode-cfg enable
 set ipv4-split-exclude <string>
 set ipv6-split-exclude <string>
 next
end
```

## IPsec VPN with external DHCP service

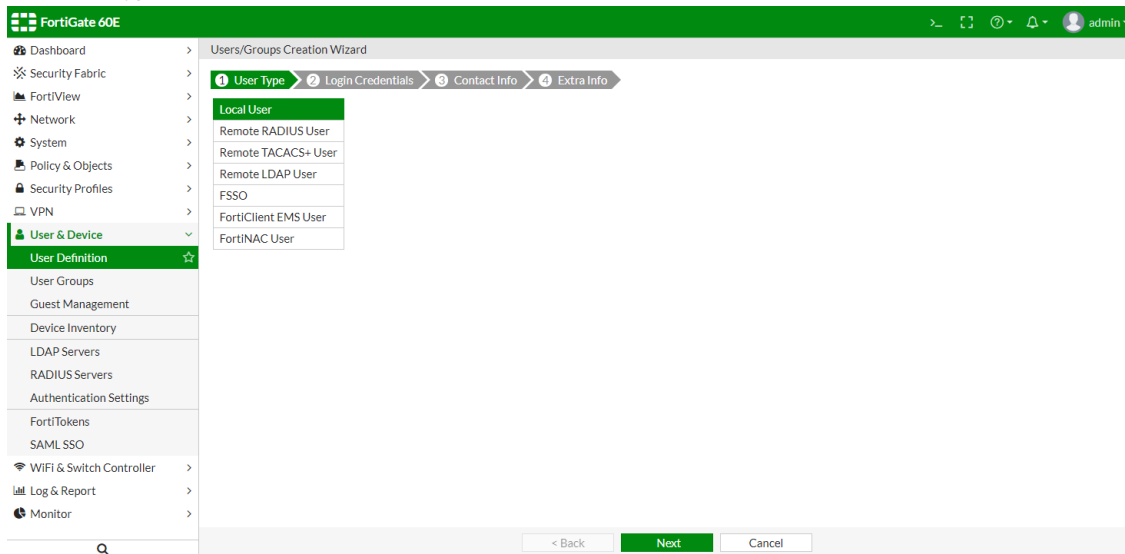
You can use an external DHCP server to assign IP addresses to your IPsec VPN clients. This is a common scenario found in enterprises where all DHCP leases need to be managed centrally.

In this example, the DHCP server assigns IP addresses in the range of 172.16.6.100 to 172.16.6.120. The server is attached to internal2 on the FortiGate and has an IP address of 192.168.3.70.



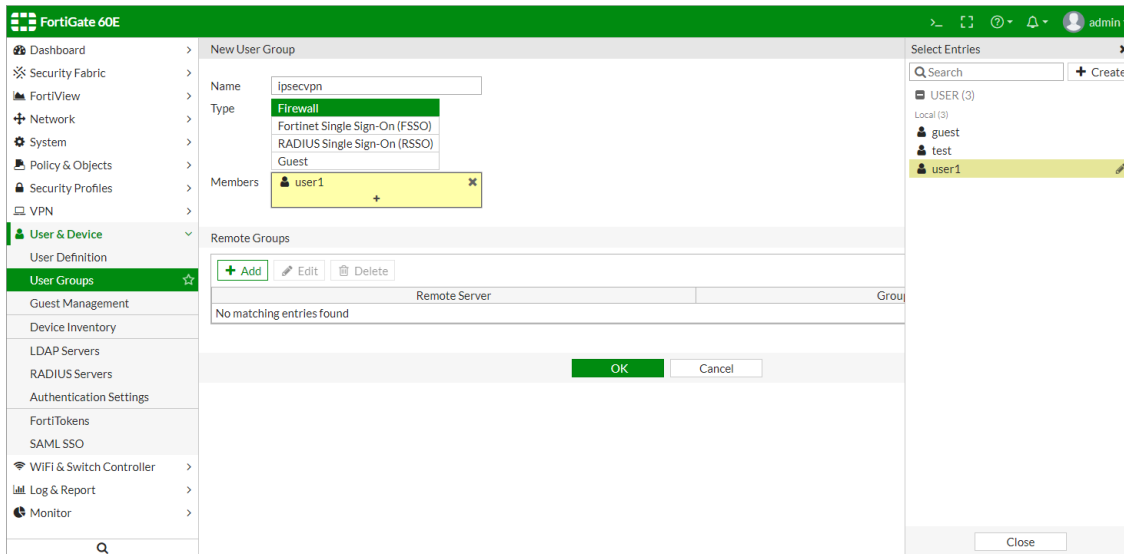
To configure a DHCP server to assign IP addresses to IPsec VPN clients:

1. Create a user group for remote users:
  - a. Go to *User & Device > User Definition > Create New*.
  - b. For *User Type*, select *Local User*.



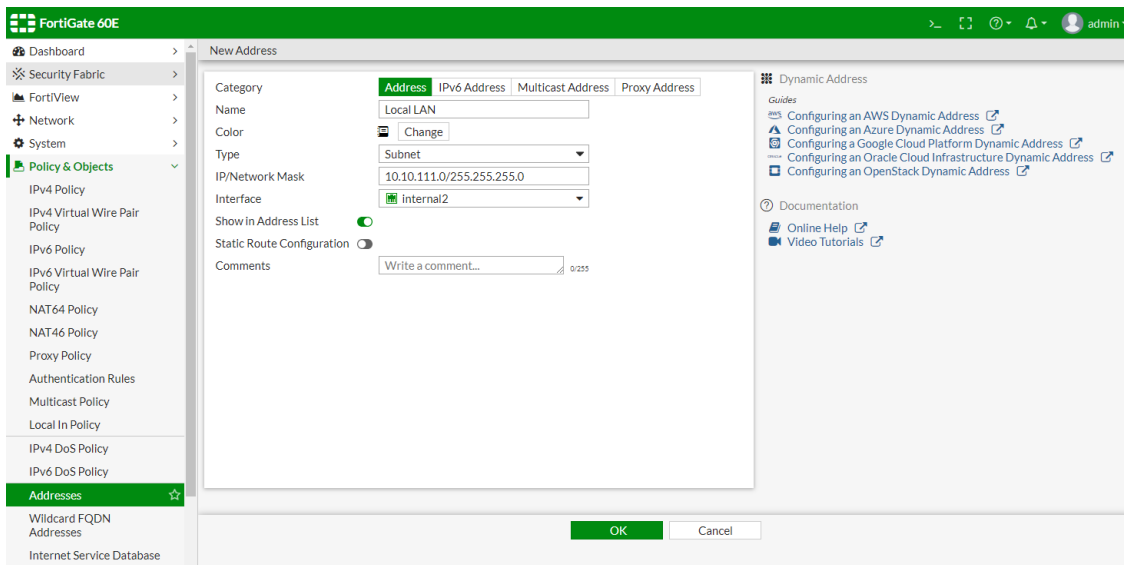
- c. Complete the wizard, and click *Submit*.
- d. Go to *User & Device > User Groups > Create New*.
- e. Create a *Firewall* user group for your remote users.
- f. For *Members*, add the user you just created.

## g. Click OK.



## 2. Add a firewall address for the local network and IPsec VPN client range:

- a. Go to *Policy & Objects* > *Addresses*.
- b. Create a new *Subnet* address for the LAN, including the IP mask and local interface (*internal2*).
- c. Click OK.



- d. Create a new *IP Range* address for the IPsec VPN client range (172.16.6.100–172.16.6.120).

## e. Click OK.

The screenshot shows the FortiGate 60E web interface. On the left is a navigation menu with categories like Dashboard, Security Fabric, FortiView, Network, System, and Policy & Objects. The 'Addresses' option under 'Policy & Objects' is selected. The main area is titled 'New Address'. It has tabs for 'Address', 'IPv6 Address', 'Multicast Address', and 'Proxy Address'. The 'Address' tab is active. Fields include: Name (ipsecvpn\_range), Color (Change), Type (IP Range), IP Range (172.16.6.100-172.16.6.120), Interface (any), Show in Address List (checked), Static Route Configuration (unchecked), and Comments (Write a comment...). At the bottom right are 'OK' and 'Cancel' buttons. On the far right, there are links for Dynamic Address guides and documentation.

## 3. Configure the IPsec VPN using a VPN tunnel in the CLI:

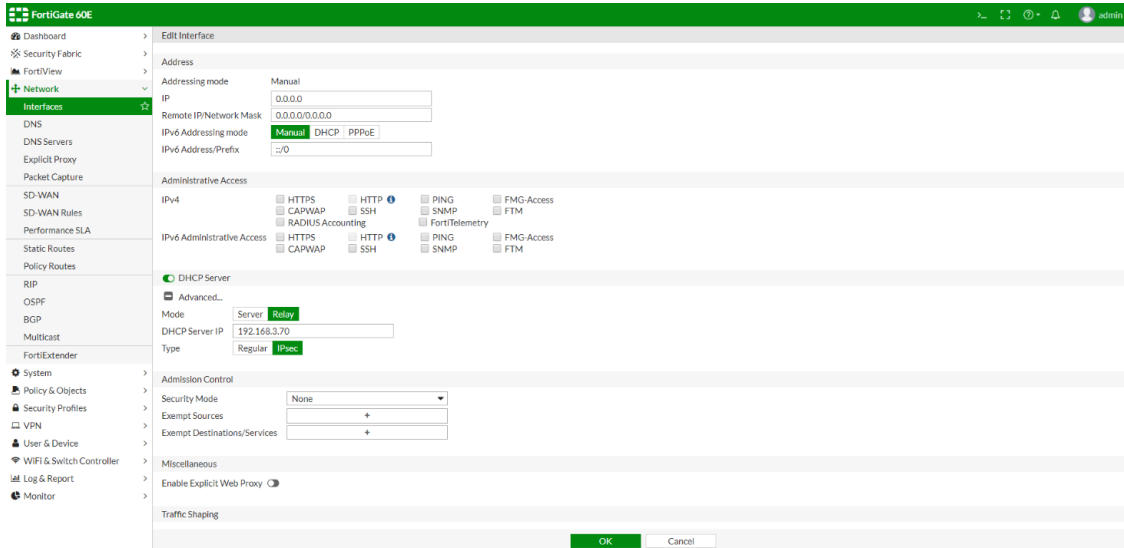
```
config vpn ipsec phase1-interface
 edit "dhcp_vpn"
 set type dynamic
 set interface "wan1"
 set mode aggressive
 set peertype any
 set net-device disable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set dpd on-idle
 set dhgrp 5
 set xauthtype auto
 set authusrgrp "ipsecvpn"
 set psksecret <xxxxxx>
 set dpd-retryinterval 60
 next
end

config vpn ipsec phase2-interface
 edit "toclient"
 set phase1name "dhcp_vpn"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
 set dhgrp 5
 set dhcp-ipsec enable
 next
end
```

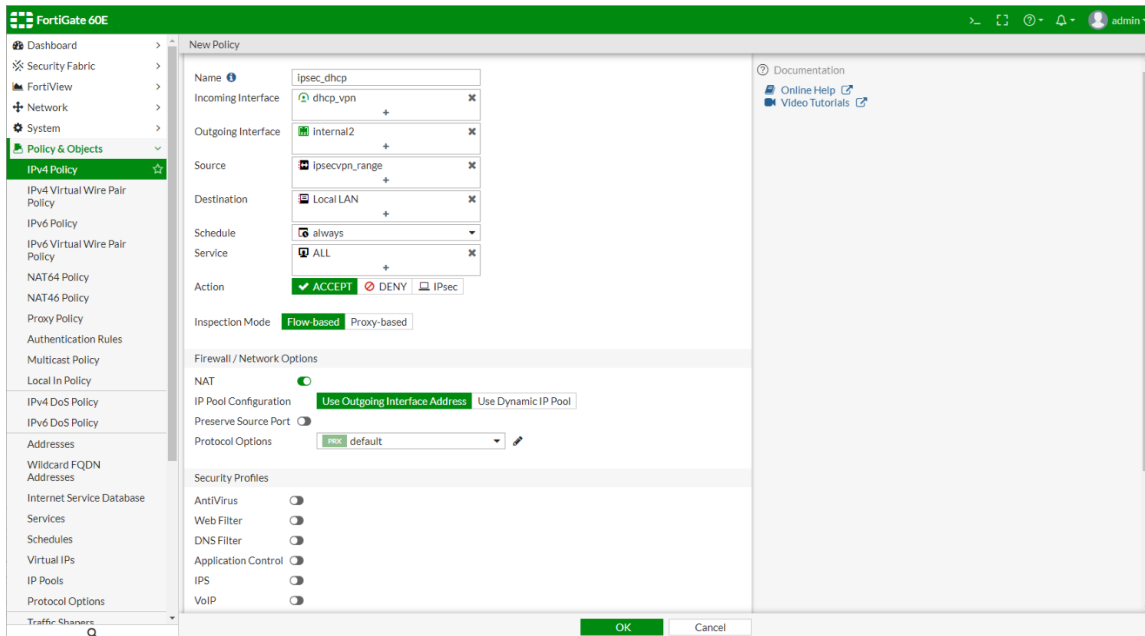
## 4. Configure the IPsec VPN interface:

- a. Go to **Network > Interfaces** and edit the newly created IPsec VPN interface.
- b. Enable the **DHCP Server**.

- c. Expand *Advanced* and change the *Mode* to *Relay*.
- d. Enter the external DHCP server IP address (192.168.3.70).
- e. Change the *Type* to *IPsec*.
- f. Click **OK**.

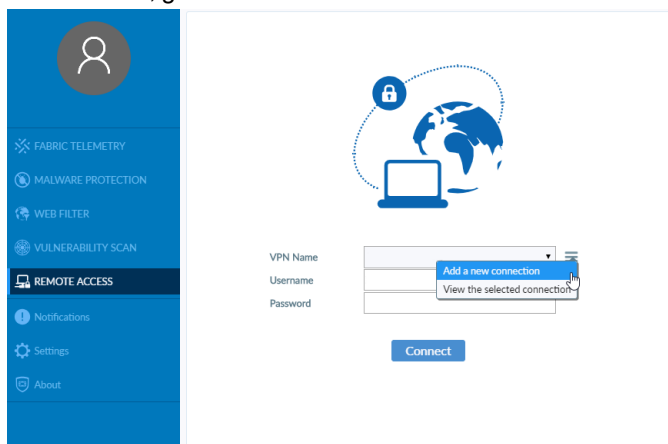


5. Create a security policy for access to the local network:
  - a. Go to *Policy & Objects* > *IPv4 Policy* > *Create New*.
  - b. Configure the following parameters:
    - i. Set the *Incoming Interface* to the tunnel interface created in step 3 (*dhcp\_vpn*).
    - ii. Set the *Outgoing Interface* (*internal2*).
    - iii. Set the *Source* to the IPsec VPN client range defined in step 2 (*ipsecvpn\_range*).
    - iv. Set the *Destination* to the subnet address defined in step 2 (*Local LAN*).
    - v. Set the *Service* to *ALL*.
  - c. Click **OK**.

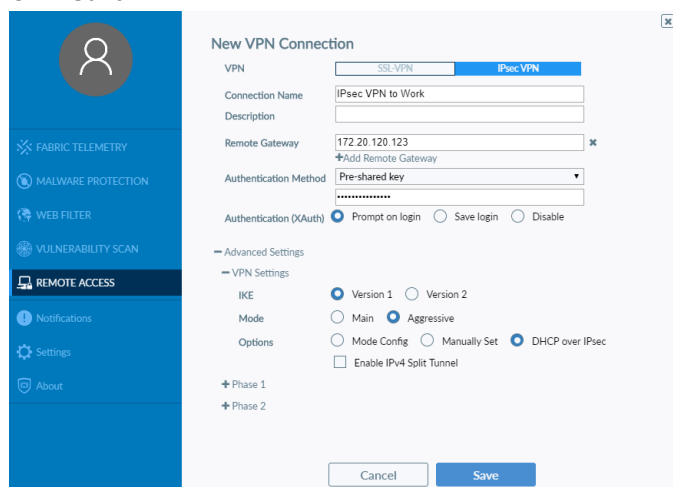


## 6. Configure FortiClient:

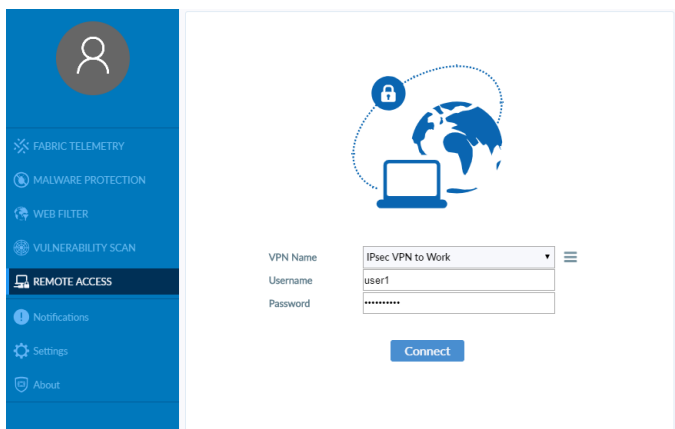
- a. In FortiClient, go to **REMOTE ACCESS > Add a new connection**.



- b. Configure the following parameters:
  - i. Set the *VPN type* to *IPsec VPN*.
  - ii. Enter a connection name.
  - iii. Set the *Remote Gateway* to the FortiGate external IP address.
  - iv. Set the *Authentication Method* to *Pre-shared key* and enter the key below.
  - v. Expand the *Advanced Settings > VPN Settings* and for *Options*, select *DHCP over IPsec*.
  - vi. Click **Save**.



- c. Select the new connection, and enter the user name and password.

d. Click *Connect*.

Once the connection is established, the external DHCP server assigns the user an IP address and FortiClient displays the connection status, including the IP address, connection duration, and bytes sent and received.

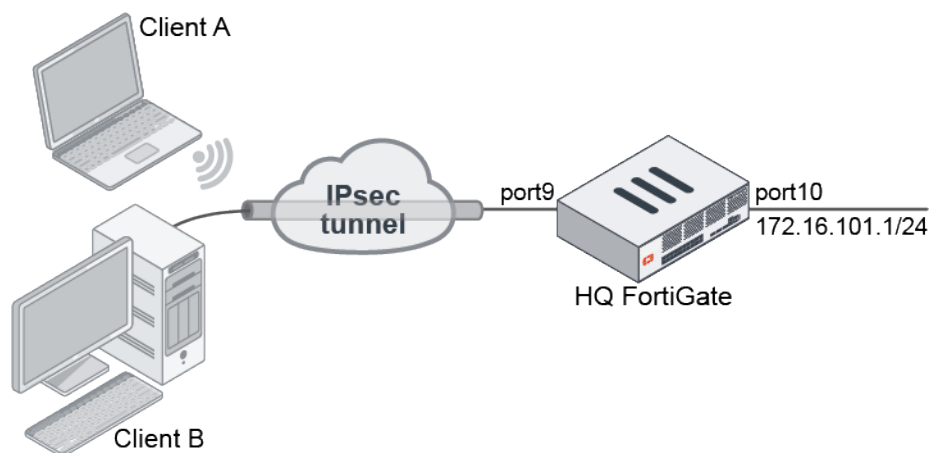
## Verification

1. In FortiOS, go to *Monitor > IPsec Monitor* and verify that the tunnel *Status* is *Up*.
2. Go to *Log & Report > Forward Traffic* and verify the *Sent / Received* column displays the traffic flow through the tunnel.

## L2TP over IPsec

This is an example of L2TP over IPsec.

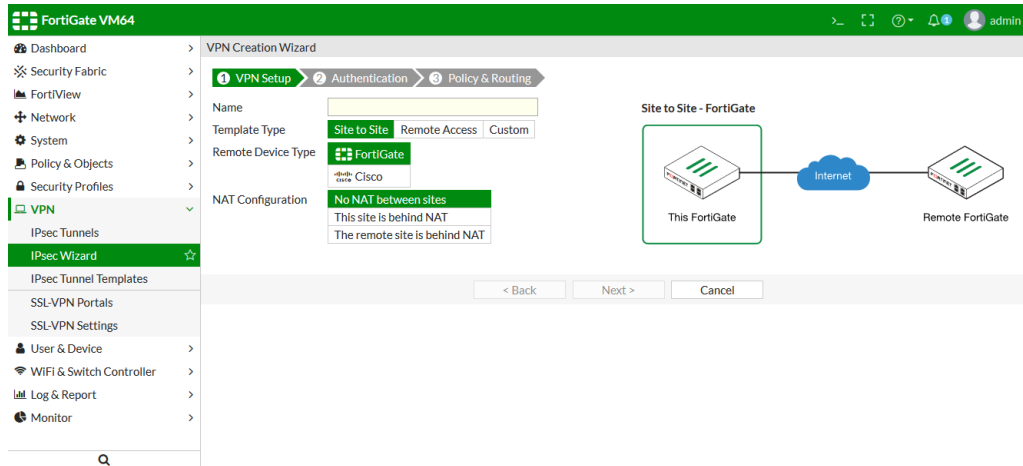
This example uses a locally defined user for authentication, a Windows PC or Android tablet as the client, and `net-device` is set to enable in the `phase1-interface` settings. If `net-device` is set to disable, only one device can establish an L2TP over IPsec tunnel behind the same NAT device.





## To configure L2TP over an IPsec tunnel using the GUI:

1. Go to **VPN > IPsec Wizard**.



2. Enter a **VPN Name**. In this example, *L2tpolPsec*.
3. Configure the following settings for **VPN Setup**:
  - a. For **Template Type**, select *Remote Access*.
  - b. For **Remote Device Type**, select *Native* and *Windows Native*.
  - c. Click **Next**.
4. Configure the following settings for **Authentication**:
  - a. For **Incoming Interface**, select *port9*.
  - b. For **Authentication Method**, select *Pre-shared Key*.
  - c. In the **Pre-shared Key** field, enter *your-psk* as the key.
  - d. For **User Group**, select *L2tpusergroup*.
  - e. Click **Next**.
5. Configure the following settings for **Policy & Routing**:
  - a. From the **Local Interface** dropdown menu, select *port10*.
  - b. Configure the **Local Address** as *172.16.101.0*.
  - c. Configure the **Client Address Range** as *10.10.10.1-10.10.10.100*.
  - d. Leave the **Subnet Mask** at its default value.
  - e. Click **Create**.

## To configure L2TP over an IPsec tunnel using the CLI:

1. Configure the WAN interface and static route on HQ.

```
config system interface
 edit "port9"
 set alias "WAN"
 set ip 22.1.1.1 255.255.255.0
 next
 edit "port10"
 set alias "Internal"
 set ip 172.16.101.1 255.255.255.0
 next
end
config router static
```

```
 edit 1
 set gateway 22.1.1.2
 set device "port9"
 next
end
```

## 2. Configure IPsec phase1-interface and phase2-interface on HQ.

```
config vpn ipsec phase1-interface
 edit "L2tpoIPsec"
 set type dynamic
 set interface "port9"
 set peertype any
 set proposal aes256-md5 3des-sha1 aes192-sha1
 set dpd on-idle
 set dhgrp 2
 set net-device enable
 set psksecret sample
 set dpd-retryinterval 60
 next
end
config vpn ipsec phase2-interface
 edit "L2tpoIPsec"
 set phase1name "L2tpoIPsec"
 set proposal aes256-md5 3des-sha1 aes192-sha1
 set pfs disable
 set encapsulation transport-mode
 set l2tp enable
 next
end
```

## 3. Configure a user and user group on HQ.

```
config user local
 edit "usera"
 set type password
 set passwd usera
 next
end
config user group
 edit "L2tpusergroup"
 set member "usera"
 next
end
```

## 4. Configure L2TP on HQ.

```
config vpn l2tp
 set status enable
 set eip 10.10.10.100
 set sip 10.10.10.1
 set usrgrp "L2tpusergroup"
end
```

## 5. Configure a firewall address that is applied in L2TP settings to assign IP addresses to clients once the L2TP tunnel is established.

```
config firewall address
 edit "L2TPclients"
```

```

 set type iprange
 set start-ip 10.10.10.1
 set end-ip 10.10.10.100
 next
end

```

## 6. Configure a firewall policy.

```

config firewall policy
 edit 1
 set name "Bridge_IPsec_port9_for_l2tp negotiation"
 set srcintf "L2tpoIPsec"
 set dstintf "port9"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "L2TP"
 next
 edit 2
 set srcintf "L2tpoIPsec"
 set dstintf "port10"
 set srcaddr "L2TPclients"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
 set nat enable
 next
end

```

## To view the VPN tunnel list on HQ:

```
diagnose vpn tunnel list
```

```
list all ipsec tunnel in vd 0
```

```

```

```

name=L2tpoIPsec_0 ver=1 serial=8 22.1.1.1:0->10.1.100.15:0
bound_if=4 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/216 options[00d8]=npu
create_dev no-sysctl rgwy-chg
parent=L2tpoIPsec index=0
proxyid_num=1 child_num=0 refcnt=13 ilast=0 olast=0 ad=/0
stat: rxp=470 txp=267 rxb=57192 txb=12679
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=L2tpoIPsec proto=17 sa=1 ref=3 serial=1 transport-mode add-route
src: 17:22.1.1.1-22.1.1.1:1701
dst: 17:10.1.100.15-10.1.100.15:0
SA: ref=3 options=1a6 type=00 soft=0 mtu=1470 expire=2339/0B replaywin=2048
seqno=10c esn=0 replaywin_lastseq=000001d6 itn=0
life: type=01 bytes=0/0 timeout=3585/3600
dec: spi=ca646443 esp=3des key=24 af62a0fffe85d3d534b5bfba29307aafc8bfda5c3f4650dc
ah=sha1 key=20 89b4b67688bed9be49fb86449bb83f8c8d8d7432
enc: spi=700d28a0 esp=3des key=24 5f68906eca8d37d853814188b9e29ac4913420a9c87362c9
ah=sha1 key=20 d37f901ffd0e6ee1e4fdccebc7fdcc7ad44f0a0a
dec:pkts/bytes=470/31698, enc:pkts/bytes=267/21744
npu_flag=00 npu_rgwy=10.1.100.15 npu_lgwy=22.1.1.1 npu_selid=6 dec_npuid=0 enc_npuid=0

```

```

name=L2tpoIPsec_1 ver=1 serial=a 22.1.1.1:4500->22.1.1.2:64916
bound_if=4 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/472 options[01d8]=npu
create_dev no-sysctl rgwy-chg rport-chg
parent=L2tpoIPsec index=1
proxyid_num=1 child_num=0 refcnt=17 ilast=2 olast=2 ad=/0
stat: rxp=5 txp=4 rxb=592 txb=249
dpd: mode=on-idle on=1 idle=60000ms retry=3 count=0 seqno=0
natt: mode=keepalive draft=32 interval=10 remote_port=64916
proxyid=L2tpoIPsec proto=17 sa=1 ref=3 serial=1 transport-mode add-route
src: 17:22.1.1.1-22.1.1.1:1701
dst: 17:22.1.1.2-22.1.1.2:0
SA: ref=3 options=1a6 type=00 soft=0 mtu=1454 expire=28786/0B replaywin=2048
seqno=5 esn=0 replaywin_lastseq=00000005 itn=0
life: type=01 bytes=0/0 timeout=28790/28800
dec: spi=ca646446 esp=aes key=32
ea60dfbad709b3c63917c3b7299520ff7606756ca15d2eb7cbff349b6562172e
ah=md5 key=16 2f2acfff0b556935d0aab8fc5725c8ec
enc: spi=0b514df2 esp=aes key=32
a8a92c2ed0e1fd7b6e405d8a6b9eb3be5eff573d80be3f830ce694917d634196
ah=md5 key=16 e426c33a7fe9041bdc5ce802760e8a3d
dec:pkts/bytes=5/245, enc:pkts/bytes=4/464
npu_flag=00 npu_rgwy=22.1.1.2 npu_lgwy=22.1.1.1 npu_selid=8 dec_npuid=0 enc_npuid=0

```

### To view the L2TP VPN status:

```

diagnose debug enable
diagnose vpn l2tp status

HQ # Num of tunnels: 2

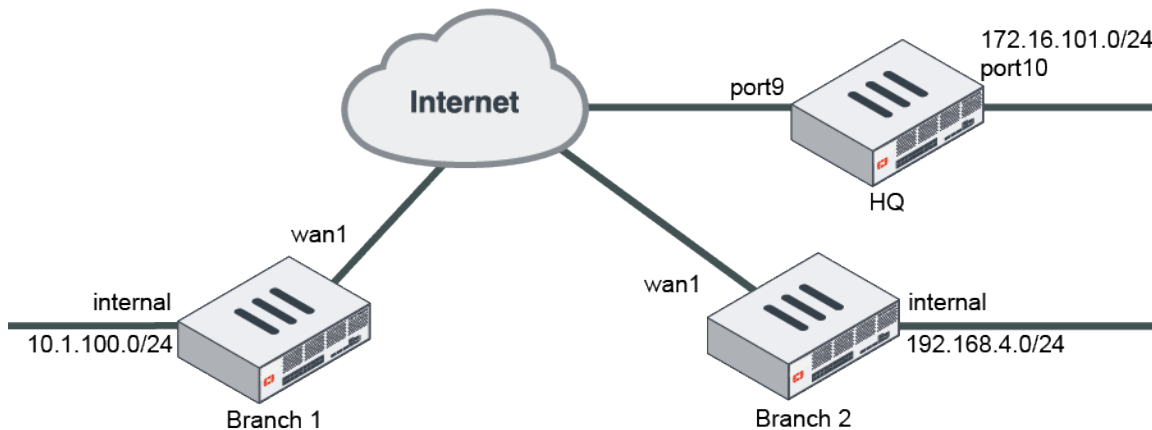
Tunnel ID = 1 (local id), 42 (remote id) to 10.1.100.15:1701
control_seq_num = 2, control_rec_seq_num = 4,
last rcv pkt = 2
Call ID = 1 (local id), 1 (remote id), serno = 0, dev=ppp1,
assigned ip = 10.10.10.2
data_seq_num = 0,
tx = 152 bytes (2), rx= 21179 bytes (205)
Tunnel ID = 3 (local id), 34183 (remote id) to 22.1.1.2:58825
control_seq_num = 2, control_rec_seq_num = 4,
last rcv pkt = 2
Call ID = 3 (local id), 18820 (remote id), serno = 2032472593, dev=ppp2,
assigned ip = 10.10.10.3
data_seq_num = 0,
tx = 152 bytes (2), rx= 0 bytes (0)

--VD 0: Startip = 10.10.10.1, Endip = 10.10.10.100
enforce-ipsec = false

```

## Tunneled Internet browsing

This is a sample configuration of tunneled internet browsing using a dialup VPN. To centralize network management and control, all branch office traffic is tunneled to HQ, including Internet browsing.



### To configure a dialup VPN to tunnel Internet browsing using the GUI:

1. Configure the dialup VPN server FortiGate at HQ:
  - a. Go to *VPN > IPsec Wizard* and configure the following settings for *VPN Setup*:
    - i. Enter a VPN name, in this example, *HQ*.
    - ii. For *Template Type*, select *Site to Site*.
    - iii. For *Remote Device Type*, select *FortiGate*.
    - iv. For *NAT Configuration*, select *The remote site is behind NAT*.
    - v. Click *Next*.
  - b. Configure the following settings for *Authentication*:
    - i. For *Incoming Interface*, select *port9*.
    - ii. For *Authentication Method*, select *Pre-shared Key*.
    - iii. In the *Pre-shared Key* field, enter *sample* as the key.
    - iv. Click *Next*.
  - c. Configure the following settings for *Policy & Routing*:
    - i. From the *Local Interface* dropdown menu, select *port10*.
    - ii. Configure the *Local Subnets* as *172.16.101.0*.
    - iii. Configure the *Remote Subnets* as *0.0.0.0/0*.
    - iv. For *Internet Access*, select *Share Local*.
    - v. For *Shared WAN*, select *port9*.
    - vi. Click *Create*.
2. Configure the dialup VPN client FortiGate at a branch:
  - a. Go to *VPN > IPsec Wizard* and configure the following settings for *VPN Setup*:
    - i. Enter a VPN name, in this example, *Branch1* or *Branch2*.
    - ii. For *Template Type*, select *Site to Site*.
    - iii. For *Remote Device Type*, select *FortiGate*.
    - iv. For *NAT Configuration*, select *The remote site is behind NAT*.
    - v. Click *Next*.

- b. Configure the following settings for *Authentication*:
  - i. For *IP Address*, select *Remote Device* and enter 22.1.1.1.
  - ii. For *Outgoing Interface*, select wan1.
  - iii. For *Authentication Method*, select *Pre-shared Key*.
  - iv. In the *Pre-shared Key* field, enter *sample* as the key.
  - v. Click *Next*.
- c. Configure the following settings for *Policy & Routing*:
  - i. From the *Local Interface* dropdown menu, select *internal*.
  - ii. Configure the *Local Subnets* as 10.1.100.0/192.1684.0.
  - iii. Configure the *Remote Subnets* as 0.0.0.0/0.
  - iv. For *Internet Access*, select *Use Remote*.
  - v. Configure the *Local Gateway* to 15.1.1.1/13.1.1.1.
  - vi. Click *Create*.

### To configure a dialup VPN to tunnel Internet browsing using the CLI:

1. Configure the WAN interface and static route on the FortiGate at HQ.

```
config system interface
 edit "port9"
 set alias "WAN"
 set ip 22.1.1.1 255.255.255.0
 next
 edit "port10"
 set alias "Internal"
 set ip 172.16.101.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 22.1.1.2
 set device "port9"
 next
end
```

2. Configure IPsec phase1-interface and phase2-interface configuration at HQ.

```
config vpn ipsec phase1-interface
 edit "HQ"
 set type dynamic
 set interface "port9"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set dpd on-idle
 set psksecret sample
 set dpd-retryinterval 60
 next
end
config vpn ipsec phase2-interface
 edit "HQ"
 set phaselname "HQ"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
```

```
 next
end
```

### 3. Configure the firewall policy at HQ.

```
config firewall policy
 edit 1
 set srcintf "HQ"
 set dstintf "port9" "port10"
 set srcaddr "10.1.100.0" "192.168.4.0"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set nat enable
 next
end
```

### 4. Configure the WAN interface and static route on the FortiGate at the branches.

#### a. Branch1.

```
config system interface
 edit "wan1"
 set ip 15.1.1.2 255.255.255.0
 next
 edit "internal"
 set ip 10.1.100.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 15.1.1.1
 set device "wan1"
 next
end
```

#### b. Branch2.

```
config system interface
 edit "wan1"
 set ip 13.1.1.2 255.255.255.0
 next
 edit "internal"
 set ip 192.168.4.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 13.1.1.1
 set device "wan1"
 next
end
```

### 5. Configure IPsec phase1-interface and phase2-interface configuration at the branches.

#### a. Branch1.

```
config vpn ipsec phase1-interface
 edit "branch1"
```

```
 set interface "wan1"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set dpd on-idle
 set remote-gw 22.1.1.1
 set psksecret sample
 set dpd-retryinterval 5
 next
end
config vpn ipsec phase2-interface
 edit "branch1"
 set phase1name "branch1"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
 set auto-negotiate enable
 set src-subnet 10.1.100.0 255.255.255.0
 next
end
```

**b. Branch2.**

```
config vpn ipsec phase1-interface
 edit "branch2"
 set interface "wan1"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set dpd on-idle
 set remote-gw 22.1.1.1
 set psksecret sample
 set dpd-retryinterval 5
 next
end
config vpn ipsec phase2-interface
 edit "branch2"
 set phase1name "branch2"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
aes256gcm chacha20poly1305
 set auto-negotiate enable
 set src-subnet 192.168.4.0 255.255.255.0
 next
end
```

**6. Configure the firewall policy at the branches.**

**a. Branch1.**

```
config firewall policy
 edit 1
 set name "outbound"
 set srcintf "internal"
 set dstintf "branch1"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
```



```
next
edit 2
 set name "inbound"
 set srcintf "branch1"
 set dstintf "internal"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
next
end
```

**b. Branch2.**

```
config firewall policy
edit 1
 set name "outbound"
 set srcintf "internal"
 set dstintf "branch2"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
next
edit 2
 set name "inbound"
 set srcintf "branch2"
 set dstintf "internal"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
next
end
```

**7. Configure the static routes at the branches.**

**a. Branch1.**

```
config router static
edit 2
 set dst 22.1.1.1/32
 set gateway 15.1.1.1
 set device "wan1"
 set distance 1
next
edit 3
 set device "branch1"
 set distance 5
next
end
```

**b. Branch2.**

```
config router static
edit 2
```

```

 set dst 22.1.1.1/32
 set gateway 13.1.1.1
 set device "wan1"
 set distance 1
 next
 edit 3
 set device "branch2"
 set distance 5
 next
end

```

8. Optionally, view the VPN tunnel list on a branch with the `diagnose vpn tunnel list` command:

```

list all ipsec tunnel in vd 0

name=branch1 ver=1 serial=2 15.1.1.2:0->22.1.1.1:0
bound_if=7 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu create_
dev frag-rfc accept_traffic=1

proxyid_num=1 child_num=1 refcnt=19 ilast=0 olast=0 ad=r/2
stat: rxp=1 txp=1661 rxb=65470 txb=167314
dpd: mode=on-idle on=1 idle=5000ms retry=3 count=0 seqno=2986
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=branch1 proto=0 sa=1 ref=5 serial=1 auto-negotiate adr
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=697/0B replaywin=1024
seqno=13a esn=0 replaywin_lastseq=00000000 itn=0
life: type=01 bytes=0/0 timeout=2368/2400
dec: spi=c53a8f7e esp=aes key=16 ecee0cd48664d903d3d6822b1f902fd2
ah=sha1 key=20 2440a189126c222093ca9acd8b37127285f1f8a7
enc: spi=6e3636fe esp=aes key=16 fdad20bcc96f74ae9885e824d3efa29d
ah=sha1 key=20 70c0891c769ad8007eaf31a39978ffbc73242d0
dec:pkts/bytes=0/16348, enc:pkts/bytes=313/55962
npu_flag=03 npu_rgw=22.1.1.1 npu_lgwy=15.1.1.2 npu_selid=1 dec_npuid=1 enc_npuid=1

```

9. Optionally, view static routing table on a branch with the `get router info routing-table static` command:

```

Routing table for VRF=0
S* 0.0.0.0/0 [5/0] is directly connected, branch1
S* 22.1.1.1/32 [1/0] via 15.1.1.1, wan1

```

## Dialup IPsec VPN with certificate authentication

In a dialup IPsec VPN setup, a company may choose to use X.509 certificates as their authentication solution for remote users. This method includes the option to verify the remote user using a user certificate, instead of a username and password. This method can be simpler for end users.

Administrators need to issue unique user certificates to each user for remote access management. The user certificate can be verified by the subject field, common name, or the principal name in the Subject Alternative Name (SAN) field.

### Subject field verification

This is the basic method that verifies the subject string defined in the PKI user setting matches a substring in the subject field of the user certificate. For example:

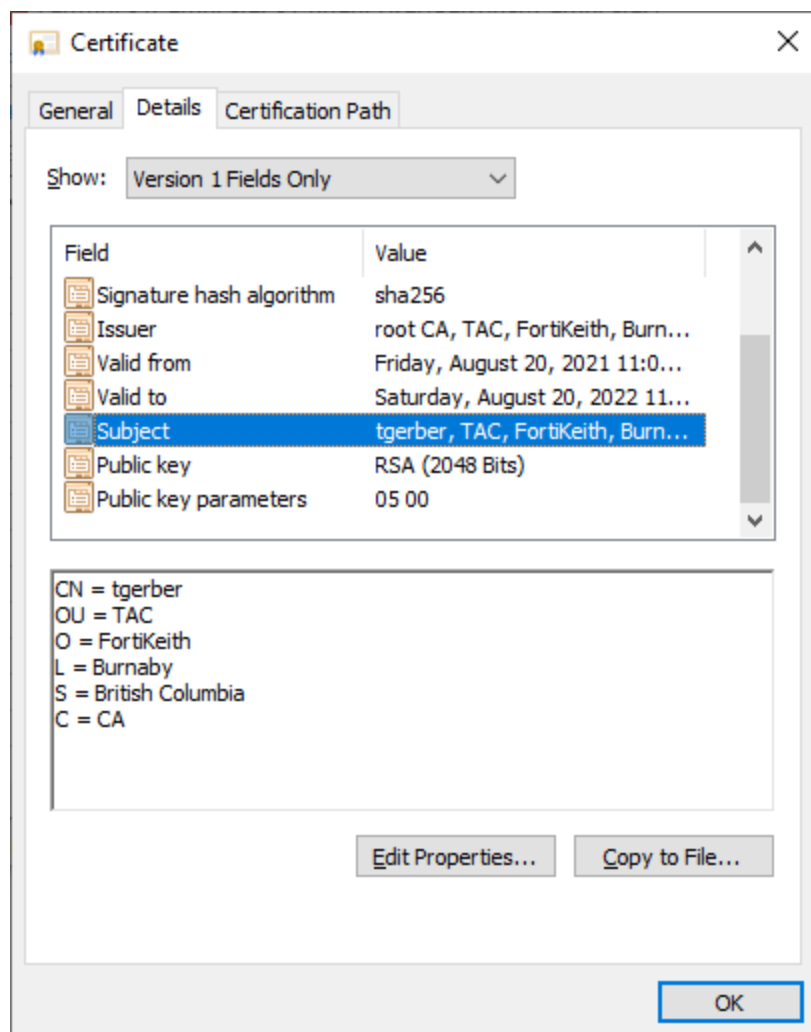
```
config user peer
 edit "tgerber"
 set ca "CA_Cert_2"
 set subject "CN=tgerber"
 next
end
```

## Common name verification

In this method, administrators can define the CN string to match the common name (CN) in the subject field of the certificate. For example:

```
config user peer
 edit "tgerber"
 set ca "CA_Cert_2"
 set cn "tgerber"
 next
end
```

The matching certificate looks like the following:



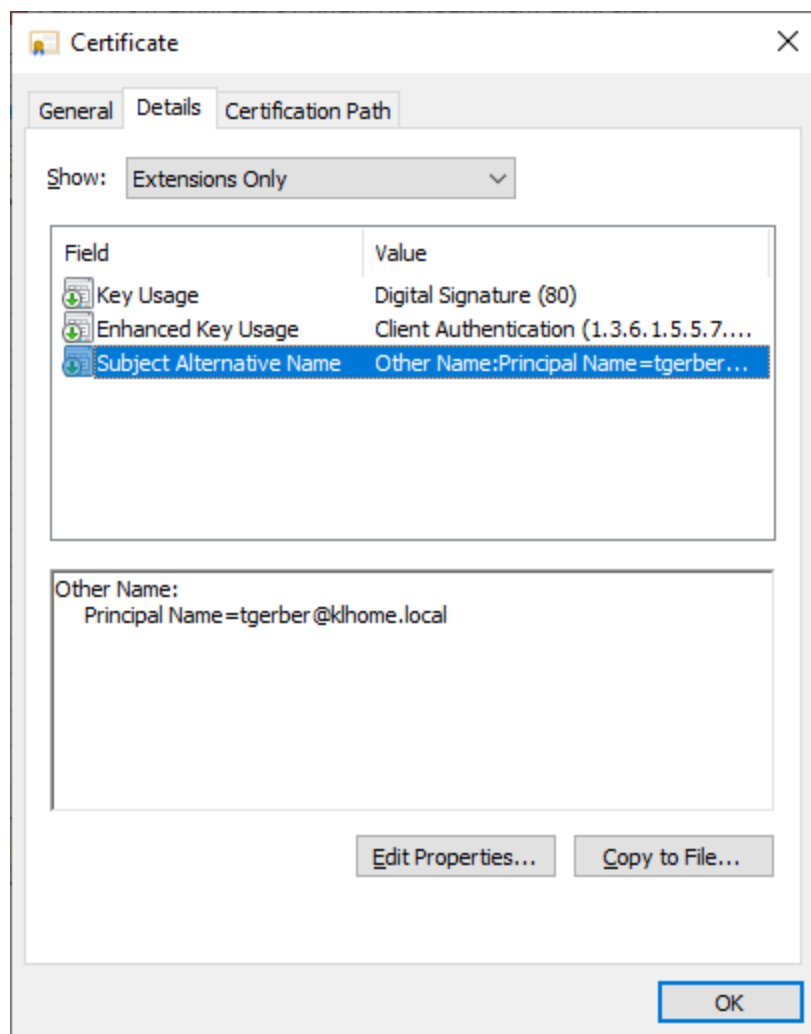
A PKI user must be created on the FortiGate for each remote user that connects to the VPN with a unique user certificate.

### Principal name with LDAP integration

In this method, the PKI user setting references an LDAP server. When `ldap-mode` is set to `principal-name`, the UPN in the user certificate's SAN field is used to look up the user in the LDAP directory. If a match is found, then authentication succeeds. For example:

```
config user peer
 edit "ldap-peer"
 set ca "CA_Cert_2"
 set ldap-server "WIN2K16-KLHOME-LDAPS"
 set ldap-mode principal-name
 next
end
```

The matching certificate looks like the following:



This method is more scalable because only one PKI user needs to be created on the FortiGate. Remote users connect with their unique user certificate that are matched against users in the LDAP server.

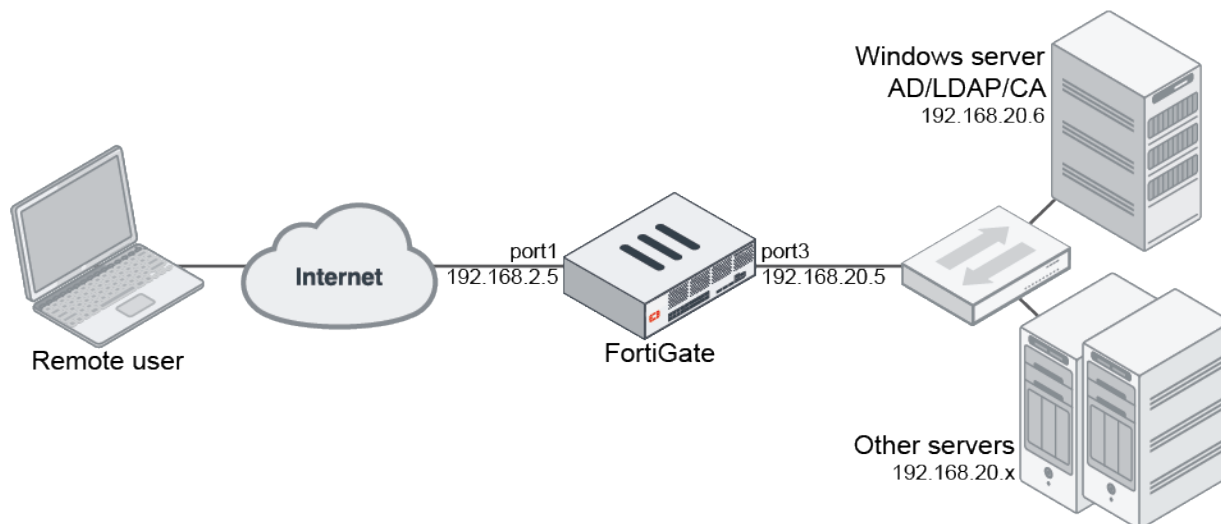
## Certificate management

Dialup IPsec VPN with certificate authentication requires careful certificate management planning. Assuming that a company's private certificate authority (CA) is used to generate and sign all the certificates, the following certificates are needed:

Certificate type	Description
Server certificate	The server certificate is used to identify the FortiGate IPsec dialup gateway. A CSR can be generated on the FortiGate and signed by the CA, or the CA can generate the private and public keys and export the certificate package to the FortiGate.
User certificate	The user certificate is generated and signed by the CA with unique CNs in the subject field and/or unique Principal Names in the SAN field. They are used to identify the user that is connecting to the VPN. User certificates must be installed on client machines.
CA certificate	The root CA certificate, and any subordinate CA that signed the actual user and server certificates, must be imported into the FortiGate and client machines. The CA certificate is used to verify the certificate chain of the server and user certificates.

## Example

In this example, a dialup IPsec VPN tunnel is configured with certificate authentication using the subject field verification method and the LDAP integration method.



The company CA, named root CA, signs all the server and user certificates. The user, tgerber@klhome.local, has a user certificate signed by root CA installed on their endpoint. The corresponding user account is also present under the company's Active Directory.

There are five major steps to configure this example:

1. [Importing the certificates](#)
2. [Configuring user authentication](#)
3. [Configuring the VPN](#)

4. [Configuring FortiClient and the endpoints](#)
5. [Testing and verifying the certificate authentication](#)

### Importing the certificates

The server certificate and CA certificate need to be imported into the FortiGate.

#### To import the server certificate:

1. Go to *System > Certificates* and select *Import > Local Certificate*.
2. For *Type*, select *PKCS #12 Certificate*.
3. Upload the key file exported from the CA and enter the password.
4. Click *OK*. The certificate now appears in the *Local Certificate* section.

#### To import the CA certificate:

1. Go to *System > Certificates* and select *Import > CA Certificate*.
2. For *Type*, select *File*.
3. Upload the CA certificate (usually a .CRT file). This certificate only contains the public key.
4. Click *OK*. The certificate now appears in the *Remote CA Certificate* section.



If any subordinate CA is involved in signing the certificates, you need to import its certificate.

---

### Configuring user authentication

FortiGate PKI users do not appear in the GUI until at least one PKI user has been created in the CLI. The following instructions create the PKI users in the CLI.

#### To configure PKI users for subject field verification:

1. Create the PKI user and choose the CA certificate that was imported (if the certificate was signed by a subordinate CA, choose the subordinate CA's certificate):

```
config user peer
 edit "tgerber"
 set ca "CA_Cert_2"
 set subject "CN=tgerber"
 next
end
```

For an example of CN field matching, see [Common name verification](#).

2. Create additional users as needed.
3. Place the users into a peer group:

```
config user peergrp
 edit "pki-users"
 set member "tgerber" <user> ... <user>
 next
end
```

## To configure PKI users for LDAP integration:

### 1. Configure the LDAP server that users connect to for authentication:

```
config user ldap
 edit "WIN2K16-KLHOME-LDAPS"
 set server "192.168.20.6"
 set cnid "sAMAccountName"
 set dn "dc=KLHOME,dc=local"
 set type regular
 set username "KLHOME\\Administrator"
 set password *****
 set secure ldaps
 set ca-cert "CA_Cert_1"
 set port 636
 next
end
```

### 2. Configure the PKI user to reference the LDAP server using the CA certificate that was imported:

```
config user peer
 edit "ldap-peer"
 set ca "CA_Cert_2"
 set ldap-server "WIN2K16-KLHOME-LDAPS"
 set ldap-mode principal-name
 next
end
```

### 3. Place the user into a peer group:

```
config user peergrp
 edit "pki-ldap"
 set member "ldap-peer"
 next
end
```

## Configuring the VPN

To configure the VPN, the address objects must be defined first so they can be used in the VPN and policy configurations. In this example, the VPN is configured in custom mode to define the authentication settings.

## To configure the address objects:

### 1. Create the address range for the dialup clients:

- Go to *Policy & Objects > Addresses* and click *Create New > Address*.
- For *Name*, enter *remote-user-range*.
- For *Type*, select *IP Range* and enter *172.18.200.10-172.18.200.99* in the *IP Range* field.
- Click *OK*.

### 2. Create the address subnet for the destination 192.168.20.0/24:

- Click *Create New > Address*.
- For *Name*, enter *192.168.20.0*.
- For *Type*, select *Subnet* and enter *192.168.20.0/24* in the *IP/Netmask* field.
- Click *OK*.

**To configure the IPsec dialup tunnel:**

1. Go to *VPN > IPsec Tunnels* and click *Create New > IPsec Tunnel*.
2. Enter a name for the tunnel, *Dialup-cert\_0*.
3. For *Template type*, select *Custom* then click *Next*.
4. In the *Network* section, enter the following:

<b>Remote Gateway</b>	<i>Dialup User</i>
<b>Interface</b>	<i>port1</i>
<b>Mode Config</b>	Enable
<b>Assign IP From</b>	<i>Range</i>
<b>IPv4 mode config &gt; Client Address Range</b>	<i>172.18.200.10-172.18.200.99</i>
<b>Enable IPv4 Split Tunnel</b>	Enable
<b>Accessible Networks</b>	<i>192.168.20.0</i>

5. In the *Authentication* section, enter the following:

<b>Method</b>	<i>Signature</i>
<b>Certificate Name</b>	Select the server certificate that was imported.
<b>Mode</b>	<i>Aggressive</i>
<b>Peer Options &gt; Accept Types</b>	<i>Peer certificate group</i>
<b>Peer Options &gt; Peer certificate group</b>	Select the group based on the preferred method: <ul style="list-style-type: none"> <li>• For subject verification, select <i>pki-users</i>.</li> <li>• For LDAP integration, select <i>pki-ldap</i>.</li> </ul>

When IKEv1 is used, aggressive mode should be selected so that the connecting endpoint will provide its peer ID in the first message of the IKE exchange. The peer identifier allows the FortiGate to match the correct tunnel when multiple dialup tunnels are defined.

6. For *Phase 2 Selectors*, leave the local and remote selectors as *0.0.0.0/0.0.0.0*.
7. Click *OK*.

**To configure the firewall policy:**

1. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
2. Configure the following:

<b>Name</b>	Enter a policy name.
<b>Incoming interface</b>	<i>Dialup-cert_0</i>
<b>Outgoing Interface</b>	<i>port3</i>
<b>Source</b>	<i>remote-user-range</i>
<b>Destination</b>	<i>192.168.20.0</i>



<b>Schedule</b>	<i>always</i>
<b>Service</b>	<i>ALL</i>
<b>Action</b>	<i>ACCEPT</i>

3. Configure the other settings as needed.
4. Click *OK*.

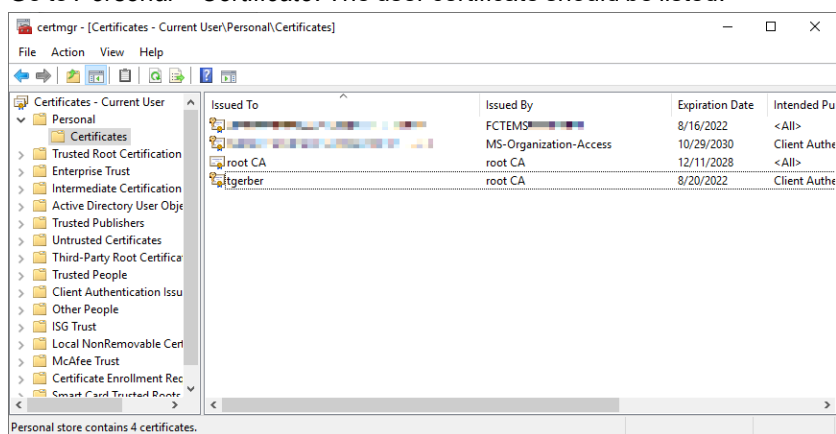
## Configuring FortiClient and the endpoints

The following example is configured on a Windows PC with FortiClient 7.0.0. Other configurations may differ slightly.

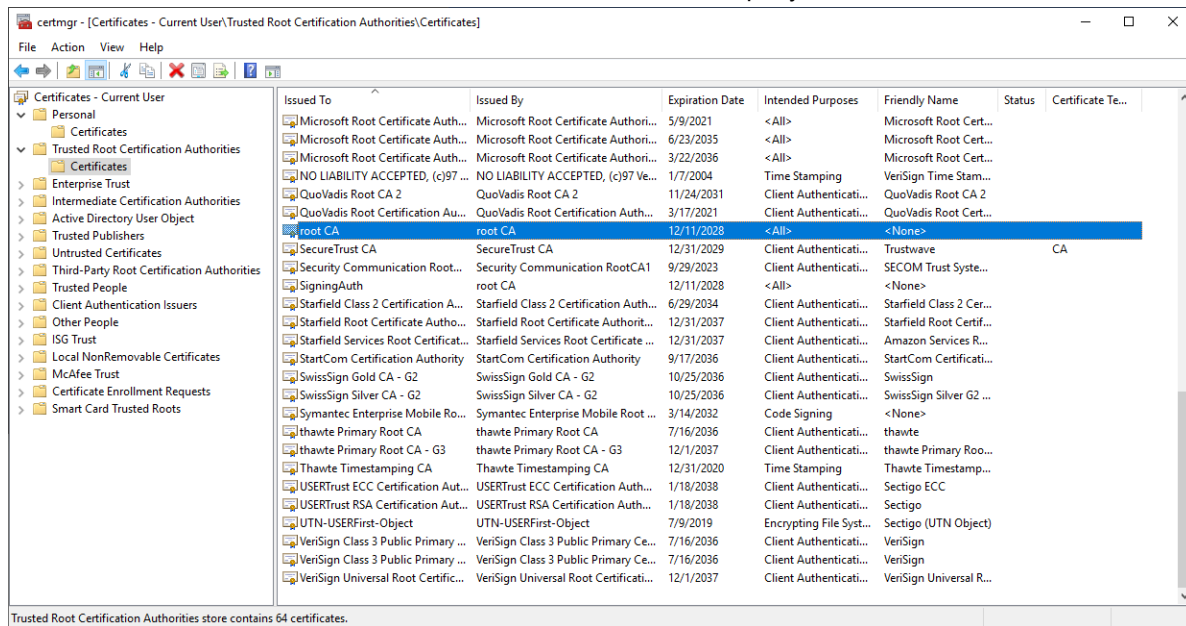
The user certificate and CA certificate must be installed on the endpoint device. They may be pushed by the administrator through group policies or another method. This example assumes that the user certificate and CA certificate are already installed on the endpoint.

### To verify the user and CA certificates:

1. Open the Windows certificate manager (certmgr):
  - a. In the Control Panel, type *Manage user certificate* in the search box.
  - b. Click the result, *Manage user certificates*.
2. Go to *Personal > Certificate*. The user certificate should be listed.



3. Go to *Trusted Root Certification Authorities > Certificates*. The company CA certificate should be listed.



### To configure the FortiClient endpoint settings:

- In FortiClient, click the *Remote Access* tab and add a new connection:
  - If there are no existing connections, click *Configure VPN*.
  - If there are existing connections, click the menu icon and select *Add a new connection*.
- Configure the following:

<b>VPN</b>	<i>IPsec VPN</i>
<b>Connection Name</b>	<i>Dialup-cert_0</i>
<b>Remote Gateway</b>	<i>192.168.2.5</i>
<b>Authentication Method</b>	<i>X.509 Certificate</i> Select the user certificate, <i>tgerber/root CA</i> , from the dropdown.
<b>Authentication (XAuth)</b>	<i>Disable</i>

- Click *Save*.

### Testing and verifying the certificate authentication

- On the client PC, open FortiClient and click the *Remote Access* tab.
- Select the VPN tunnel, *Dialup-cert\_0*, and click *Connect*.  
If the connection is successful, a FortiClient pop-up will appear briefly indicating that the IKE negotiation succeeded. The *Remote Access* window now displays *VPN Connected* and the associated VPN tunnel details.
- On the FortiGate, go to *Monitor > IPsec Monitor*. The monitor displays tunnel information, including the *Peer ID* containing the subject field of the user certificate.
- Go to *Log & Report > Events > VPN Events*. Several tunnel related logs are recorded.

5. The same logs can be viewed in the CLI:

```
execute log filter category 1
execute log filter field subtype vpn
execute log display
7: date=2021-08-23 time=15:53:08 eventtime=1629759188862005740 tz="-0700"
logid="0101037138" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec
connection status changed" msg="IPsec connection status change" action="tunnel-up"
remip=192.168.2.1 locip=192.168.2.5 remport=64916 locport=4500 outintf="port1"
cookies="19f05ebc8c2f7a0d/7716190005538db5" user="C = CA, ST = British Columbia, L =
Burnaby, O = FortiKeith, OU = TAC, CN = tgerber" group="pki-ldap" useralt="C = CA, ST =
British Columbia, L = Burnaby, O = FortiKeith, OU = TAC, CN = tgerber" xauthuser="N/A"
xauthgroup="N/A" assignip=172.18.200.10 vpntunnel="Dialup-cert_0" tunnelip=172.18.200.10
tunnelid=3418215253 tunneltype="ipsec" duration=0 sentbyte=0 rcvdbyte=0 nextstat=0
```

6. If any issues arise during the connection, run the following debug commands to troubleshoot the issue:

```
diagnose debug application ike -1
diagnose debug application fnbamd -1
diagnose debug enable
```

## Aggregate and redundant VPN

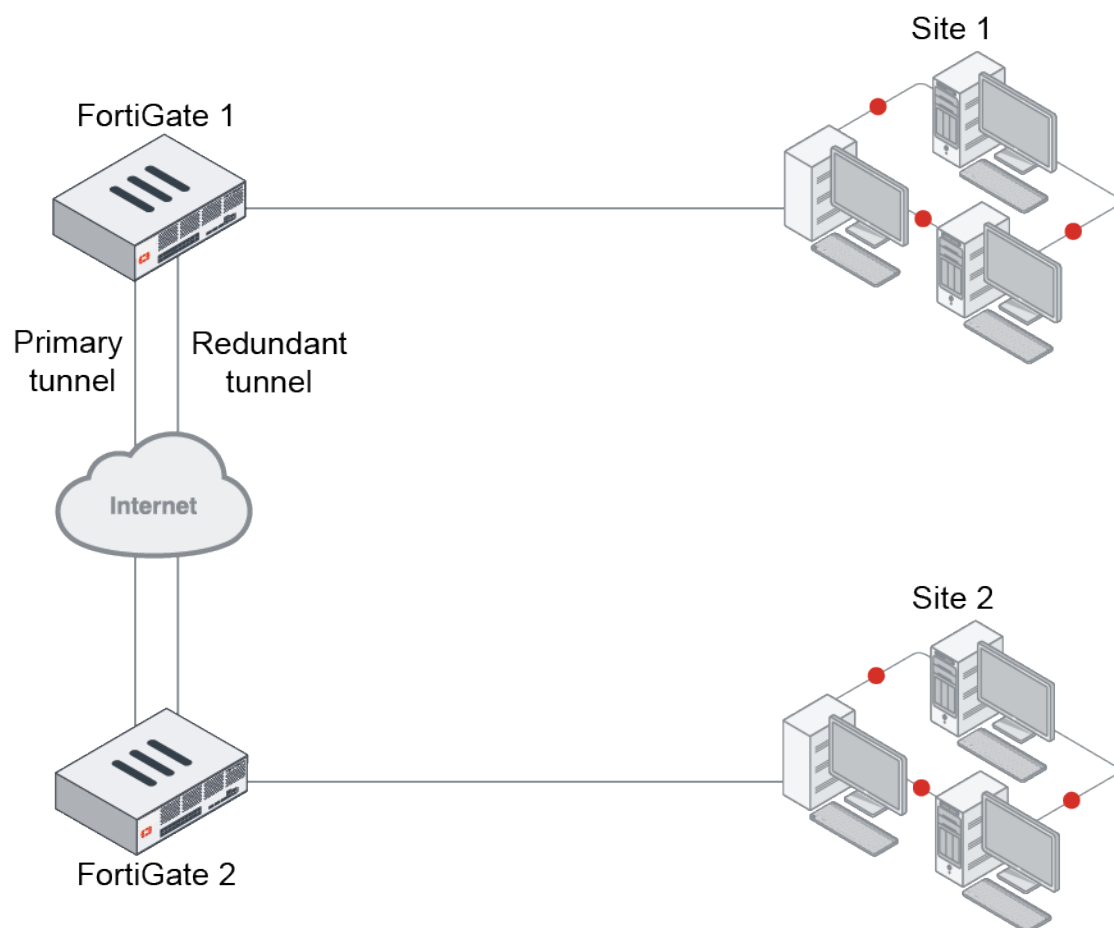
The following topics provide instructions on configuring aggregate and redundant VPNs:

- [Manual redundant VPN configuration on page 1245](#)
- [OSPF with IPsec VPN for network redundancy on page 1249](#)
- [IPsec VPN in an HA environment on page 1256](#)
- [IPsec aggregate for redundancy and traffic load-balancing on page 1262](#)
- [Per packet distribution and tunnel aggregation on page 1273](#)
- [Redundant hub and spoke VPN on page 1277](#)

### Manual redundant VPN configuration

A FortiGate with two interfaces connected to the internet can be configured to support redundant VPNs to the same remote peer. Four distinct paths are possible for VPN traffic from end to end. If the primary connection fails, the FortiGate can establish a VPN using the other connection.

## Topology



The redundant configuration in this example uses route-based VPNs. The FortiGates must operate in NAT mode and use auto-keying.

This example assumes the redundant VPNs are essentially equal in cost and capability. When the original VPN returns to service, traffic continues to use the replacement VPN until the replacement VPN fails. If the redundant VPN uses more expensive facilities, only use it as a backup while the main VPN is down.

A redundant configuration for each VPN peer includes:

- One phase 1 configuration for each path between the two peers with dead peer detection enabled
- One phase 2 definition for each phase 1 configuration
- One static route for each IPsec interface with different distance values to prioritize the routes
- Two firewall policies per IPsec interface, one for each direction of traffic

### To configure the phase 1 and phase 2 VPN settings:

1. Go to *VPN > IPsec Wizard* and select the *Custom* template.
2. Enter the tunnel name and click *Next*.

3. Enter the following phase 1 settings for path 1:

<b>Remote Gateway</b>	Static IP Address
<b>IP Address</b>	Enter the IP address of the primary interface of the remote peer.
<b>Interface</b>	Select the primary public interface of this peer.
<b>Dead Peer Detection</b>	On-Demand

4. Configure the remaining phase 1 and phase 2 settings as needed.
5. Click **OK**.
6. Repeat these steps for the remaining paths.
  - a. Path 2:

<b>Remote Gateway</b>	Static IP Address
<b>IP Address</b>	Enter the IP address of the secondary interface of the remote peer.
<b>Interface</b>	Select the primary public interface of this peer.
<b>Dead Peer Detection</b>	On-Demand

- b. Path 3:

<b>Remote Gateway</b>	Static IP Address
<b>IP Address</b>	Enter the IP address of the primary interface of the remote peer.
<b>Interface</b>	Select the secondary public interface of this peer.
<b>Dead Peer Detection</b>	On-Demand

- c. Path 4:

<b>Remote Gateway</b>	Static IP Address
<b>IP Address</b>	Enter the IP address of the secondary interface of the remote peer.
<b>Interface</b>	Select the secondary public interface of this peer.
<b>Dead Peer Detection</b>	On-Demand

### To configure the static routes:

1. Go to *Network > Static Routes* and click *Create New*.
2. In the *Destination* field, enter the subnet of the private network.
3. For *Interface*, select one of the IPsec interfaces on the local peer.
4. Enter a value for *Administrative Distance*.
5. Click **OK**.
6. Repeat these steps for the three remaining paths, and enter different values for *Administrative Distance* to prioritize the paths.

**To configure the firewall policies:**

1. Create the policies for the local primary interface:
  - a. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
  - b. Enter the following:

<b>Name</b>	Enter a name for the policy.
<b>Incoming Interface</b>	Select the local interface to the internal (private) network.
<b>Outgoing Interface</b>	Select one of the virtual IPsec interfaces.
<b>Source</b>	All
<b>Destination</b>	All
<b>Schedule</b>	Always
<b>Service</b>	All
<b>Action</b>	ACCEPT

- c. Click *OK*.
- d. Click *Create New* and configure the policy for the other direction of traffic:

<b>Name</b>	Enter a name for the policy.
<b>Incoming Interface</b>	Select one of the virtual IPsec interfaces.
<b>Outgoing Interface</b>	Select the local interface to the internal (private) network.
<b>Source</b>	All
<b>Destination</b>	All
<b>Schedule</b>	Always
<b>Service</b>	All
<b>Action</b>	ACCEPT

- e. In the policy list, drag the VPN policies above any other policies with similar source and destination addresses.
2. Repeat these steps to create the policies for the three remaining paths.

**Creating a backup IPsec interface**

A route-based VPN can be configured to act as a backup IPsec interface when the main VPN is out of service. This can only be configured in the CLI.

The backup feature works on interfaces with static addresses that have dead peer detection enabled. The `monitor` option creates a backup VPN for the specified phase 1 configuration.

**To create a backup IPsec interface:**

```
config vpn ipsec phase1-interface
edit main_vpn
set dpd on-demand
set interface port1
```

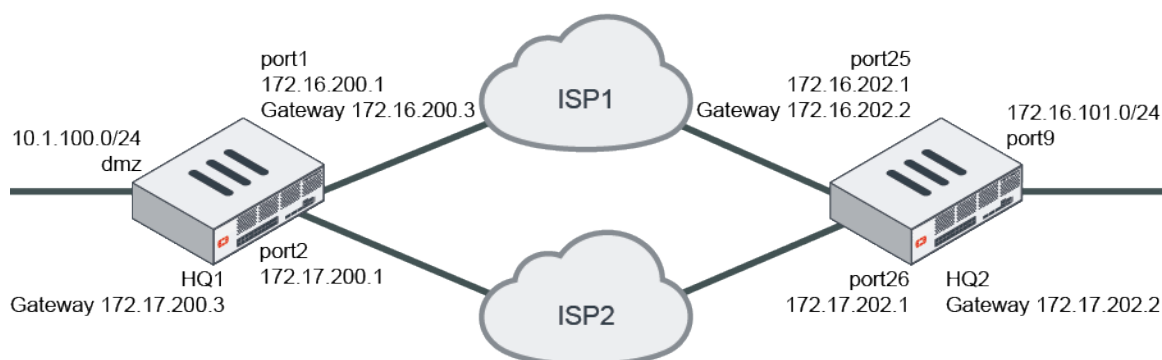
```

 set nattraversal enable
 set psksecret *****
 set remote-gw 192.168.10.8
 set type static
 next
 edit backup_vpn
 set dpd on-demand
 set interface port2
 set monitor main_vpn
 set nattraversal enable
 set psksecret *****
 set remote-gw 192.168.10.8
 set type static
 next
end

```

## OSPF with IPsec VPN for network redundancy

This is a sample configuration of using OSPF with IPsec VPN to set up network redundancy. Route selection is based on OSPF cost calculation. You can configure ECMP or primary/secondary routes by adjusting OSPF path cost.



Because the GUI can only complete part of the configuration, we recommend using the CLI.

### To configure OSPF with IPsec VPN to achieve network redundancy using the CLI:

#### 1. Configure the WAN interface and static route.

Each FortiGate has two WAN interfaces connected to different ISPs. The ISP1 link is for the primary FortiGate and the IPS2 link is for the secondary FortiGate.

##### a. Configure HQ1.

```

config system interface
 edit "port1"
 set alias to_ISP1
 set ip 172.16.200.1 255.255.255.0
 next
 edit "port2"
 set alias to_ISP2
 set ip 172.17.200.1 255.255.255.0
 next
end
config router static
 edit 1

```

```

 set gateway 172.16.200.3
 set device "port1"
 next
 edit 2
 set gateway 172.17.200.3
 set device "port2"
 set priority 100
 next
end

```

**b. Configure HQ2.**

```

config system interface
 edit "port25"
 set alias to_ISP1
 set ip 172.16.202.1 255.255.255.0
 next
 edit "port26"
 set alias to_ISP2
 set ip 172.17.202.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 172.16.202.2
 set device "port25"
 next
 edit 2
 set gateway 172.17.202.2
 set device "port26"
 set priority 100
 next
end

```

## 2. Configure the internal (protected subnet) interface.

### a. Configure HQ1.

```

config system interface
 edit "dmz"
 set ip 10.1.100.1 255.255.255.0
 next
end

```

### b. Configure HQ2.

```

config system interface
 edit "port9"
 set ip 172.16.101.1 255.255.255.0
 next
end

```

## 3. Configure IPsec phase1-interface and phase-2 interface. On each FortiGate, configure two IPsec tunnels: a primary and a secondary.

### a. Configure HQ1.

```

config vpn ipsec phase1-interface
 edit "pri_HQ2"
 set interface "port1"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.16.202.1
 set psksecret sample1
 next
end

```



```

next
edit "sec_HQ2"
 set interface "port2"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.17.202.1
 set psksecret sample2
next
end
config vpn ipsec phase2-interface
edit "pri_HQ2"
 set phaselname "pri_HQ2"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 set auto-negotiate enable
next
edit "sec_HQ2"
 set phaselname "sec_HQ2"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 set auto-negotiate enable
next
end

```

**b. Configure HQ2.**

```

config vpn ipsec phase1-interface
edit "pri_HQ1"
 set interface "port25"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.16.200.1
 set psksecret sample1
next
edit "sec_HQ1"
 set interface "port26"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.17.200.1
 set psksecret sample2
next
end
config vpn ipsec phase2-interface
edit "pri_HQ1"
 set phaselname "pri_HQ1"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 set auto-negotiate enable
next
edit "sec_HQ1"
 set phaselname "sec_HQ1"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 set auto-negotiate enable
next
end

```

**4. Configure an inbound and outbound firewall policy for each IPsec tunnel.****a. Configure HQ1.**

```
config firewall policy
edit 1
 set name "pri_inbound"
 set srcintf "pri_HQ2"
 set dstintf "dmz"
 set srcaddr "172.16.101.0"
 set dstaddr "10.1.100.0"
 set action accept
 set schedule "always"
 set service "ALL"
next
edit 2
 set name "pri_outbound"
 set srcintf "dmz"
 set dstintf "pri_HQ2"
 set srcaddr "10.1.100.0"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
next
edit 3
 set name "sec_inbound"
 set srcintf "sec_HQ2"
 set dstintf "dmz"
 set srcaddr "172.16.101.0"
 set dstaddr "10.1.100.0"
 set action accept
 set schedule "always"
 set service "ALL"
next
edit 4
 set name "sec_outbound"
 set srcintf "dmz"
 set dstintf "sec_HQ2"
 set srcaddr "10.1.100.0"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
next
end
```

**b. Configure HQ2.**

```
config firewall policy
edit 1
 set name "pri_inbound"
 set srcintf "pri_HQ1"
 set dstintf "port9"
 set srcaddr "10.1.100.0"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
next
```

```
edit 2
 set name "pri_outbound"
 set srcintf "port9"
 set dstintf "pri_HQ1"
 set srcaddr "10.1.100.0"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
next
edit 3
 set name "sec_inbound"
 set srcintf "sec_HQ1"
 set dstintf "port9"
 set srcaddr "10.1.100.0"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
next
edit 4
 set name "sec_outbound"
 set srcintf "port9"
 set dstintf "sec_HQ1"
 set srcaddr "172.16.101.0"
 set dstaddr "10.1.100.0"
 set action accept
 set schedule "always"
 set service "ALL"
next
end
5. Assign an IP address to the IPsec tunnel interface.
a. Configure HQ1.
config system interface
 edit "pri_HQ2"
 set ip 10.10.10.1 255.255.255.255
 set remote-ip 10.10.10.2 255.255.255.255
 next
 edit "sec_HQ2"
 set ip 10.10.11.1 255.255.255.255
 set remote-ip 10.10.11.2 255.255.255.255
 next
end
b. Configure HQ2.
config system interface
 edit "pri_HQ1"
 set ip 10.10.10.2 255.255.255.255
 set remote-ip 10.10.10.1 255.255.255.255
 next
 edit "sec_HQ1"
 set ip 10.10.11.2 255.255.255.255
 set remote-ip 10.10.11.1 255.255.255.255
 next
end
```

**6. Configure OSPF.****a. Configure HQ1.**

```
config router ospf
 set router-id 1.1.1.1
 config area
 edit 0.0.0.0
 next
 end
 config ospf-interface
 edit "pri_HQ2"
 set interface "pri_HQ2"
 set cost 10
 set network-type point-to-point
 next
 edit "sec_HQ2"
 set interface "sec_HQ2"
 set cost 20
 set network-type point-to-point
 next
 end
 config network
 edit 1
 set prefix 10.10.10.0 255.255.255.0
 next
 edit 2
 set prefix 10.10.11.0 255.255.255.0
 next
 edit 3
 set prefix 10.1.100.0 255.255.255.0
 next
 end
end
```

**b. Configure HQ2.**

```
config router ospf
 set router-id 2.2.2.2
 config area
 edit 0.0.0.0
 next
 end
 config ospf-interface
 edit "pri_HQ1"
 set interface "pri_HQ1"
 set cost 10
 set network-type point-to-point
 next
 edit "sec_HQ1"
 set interface "sec_HQ1"
 set cost 20
 set network-type point-to-point
 next
 end
 config network
 edit 1
 set prefix 10.10.10.0 255.255.255.0
 next
 edit 2
```

```

 set prefix 10.10.11.0 255.255.255.0
 next
 edit 3
 set prefix 172.16.101.0 255.255.255.0
 next
end
end

```

### To check VPN and OSPF states using diagnose and get commands:

1. Run the HQ1 # diagnose vpn ike gateway list command. The system should return the following:

```

vd: root/0
name: pri_HQ2
version: 1
interface: port1 11
addr: 172.16.200.1:500 -> 172.16.202.1:500
virtual-interface-addr: 10.10.10.1 -> 10.10.10.2
created: 1024s ago
IKE SA: created 1/1 established 1/1 time 0/0/0 ms
IPsec SA: created 1/3 established 1/2 time 0/5/10 ms
 id/spi: 45 d184777257b4e692/e2432f834aaf5658 direction: responder status: established
 1024-1024s ago = 0ms proposal: aes128-sha256 key: 9ed41fb06c983344-
 189538046f5ad204 lifetime/rekey: 86400/85105 DPD sent/recvd: 00000003/00000000
 vd: root/0
name: sec_HQ2
version: 1
interface: port2 12
addr: 172.17.200.1:500 -> 172.17.202.1:500
virtual-interface-addr: 10.10.11.1 -> 10.10.11.2
created: 346s ago
IKE SA: created 1/1 established 1/1 time 0/0/0 ms
IPsec SA: created 1/1 established 1/1 time 0/10/15 ms
 id/spi: 48 d909ed68636blea5/163015e73ea050b8 direction: initiator status: established
 0-0s ago = 0ms proposal: aes128-sha256 key: b9e93c156bdf4562-29db9fbafa256152
 lifetime/rekey: 86400/86099 DPD sent/recvd: 00000000/00000000

```

2. Run the HQ1 # diagnose vpn tunnel list command. The system should return the following:

```

list all ipsec tunnel in vd 0
name=pri_HQ2 ver=1 serial=1 172.16.200.1:0->172.16.202.1:0
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
 frag-rfc accept_traffic=1
proxyid_num=1 child_num=0 refcnt=14 ilast=2 olast=2 ad=/0
stat: rxp=102 txp=105 rxb=14064 txb=7816
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=3
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=pri_HQ2 proto=0 sa=1 ref=2 serial=1 auto-negotiate
 src: 0:0.0.0.0/0.0.0.0:0 dst: 0:0.0.0.0/0.0.0.0:0 SA: ref=3 options=18227 type=00
 soft=0 mtu=1438 expire=42254/0B replaywin=2048
 seqno=6a esn=0 replaywin_lastseq=00000067 itn=0
 life: type=01 bytes=0/0 timeout=42932/43200 dec: spi=1071b4ee esp=aes key=16
 032036b24a4ec88da63896b86f3a01db
 ah=sha1 key=20 3962933e24c8da21c65c13bc2c6345d643199cdf
 enc: spi=ec89b7e3 esp=aes key=16 92b1d85ef91faf695fca05843dd91626
 ah=sha1 key=20 2de99d1376506313d9f32df6873902cf6c08e454
 dec:pkts/bytes=102/7164, enc:pkts/bytes=105/14936
name=sec_HQ2 ver=1 serial=2 172.17.200.1:0->172.17.202.1:0
bound_if=12 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
 frag-rfc accept_traffic=1

```

```

proxyid_num=1 child_num=0 refcnt=14 ilast=3 olast=0 ad=/0
stat: rxp=110 txp=114 rxb=15152 txb=8428
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=3
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=sec_HQ2 proto=0 sa=1 ref=2 serial=1 auto-negotiate
src: 0:0.0.0.0/0.0.0.0:0 dst: 0:0.0.0.0/0.0.0.0:0 SA: ref=3 options=18227 type=00
soft=0 mtu=1438 expire=42927/0B replaywin=2048
seqno=2 esn=0 replaywin_lastseq=00000002 itn=0
life: type=01 bytes=0/0 timeout=42931/43200 dec: spi=1071b4ef esp=aes key=16
bcdcabdb7d1c7c695d1f2e0f5441700a
ah=sha1 key=20 e7a0034589f82eb1af41efd59d0b2565fef8d5da
enc: spi=ec89b7e4 esp=aes key=16 234240b69e61f6bdee2b4cdec0f33bea
ah=sha1 key=20 f9d4744a84d91e5ce05f5984737c2a691a3627e8
dec:pkts/bytes=1/68, enc:pkts/bytes=1/136

```

3. Run the HQ1 # get router info ospf neighbor command. The system should return the following:

```

OSPF process 0, VRF 0:
Neighbor ID Pri State Dead Time Address Interface
2.2.2.2 1. Full/ - 00:00:37 10.10.10.2 pri_HQ2
2.2.2.2 1. Full/ - 00:00:32 10.10.11.2 sec_HQ2

```

4. Run the HQ1 # get router info routing-table ospf command. The system should return the following:

```

Routing table for VRF=0
O 172.16.101.0/24 [110/20] via 10.10.10.2, pri_HQ2 , 00:03:21

```

In case the primary tunnel is down after route convergence.

5. Run the HQ1 # get router info routing-table ospf command. The system should return the following:

```

Routing table for VRF=0
O 172.16.101.0/24 [110/110] via 10.10.11.2, sec_HQ2 , 00:00:01

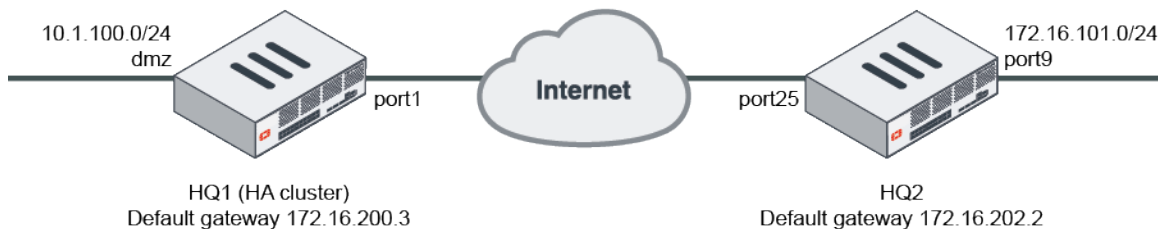
```

## IPsec VPN in an HA environment

This is a sample configuration of site-to-site IPsec VPN in an HA environment.

For this example, set up HA as described in the HA topics. When setting up HA, enable the following options to ensure IPsec VPN traffic is not interrupted during an HA failover:

- session-pickup under HA settings.
- ha-sync-esp-seqno under IPsec phase1-interface settings.



You can configure IPsec VPN in an HA environment using the [GUI](#) or [CLI](#).

In this example, the VPN name for HQ1 is "to\_HQ2", and the VPN name for HQ2 is "to\_HQ1".

**To configure IPsec VPN in an HA environment in the GUI:**

1. Set up IPsec VPN on HQ1 (the HA cluster):
  - a. Go to *VPN > IPsec Wizard* and configure the following settings for *VPN Setup*:
    - i. Enter a VPN name.
    - ii. For *Template Type*, select *Site to Site*.
    - iii. For *Remote Device Type*, select *FortiGate*.
    - iv. For *NAT Configuration*, set *No NAT between sites*.
    - v. Click *Next*.
  - b. Configure the following settings for *Authentication*:
    - i. For *Remote Device*, select *IP Address*.
    - ii. In the *IP address* field, enter *172.16.202.1*.
    - iii. For *Outgoing Interface*, select *port1*.
    - iv. For *Authentication Method*, select *Pre-shared Key*.
    - v. In the *Pre-shared Key* field, enter an example key.
    - vi. Click *Next*.
  - c. Configure the following settings for *Policy & Routing*:
    - i. From the *Local Interface* dropdown menu, select the local interface.
    - ii. Configure the *Local Subnets* as *10.1.100.0/24*.
    - iii. Configure the *Remote Subnets* as *172.16.101.0/24*.
    - iv. Click *Create*.
2. Set up IPsec VPN on HQ2:
  - a. Go to *VPN > IPsec Wizard* and configure the following settings for *VPN Setup*:
    - i. Enter a VPN name.
    - ii. For *Template Type*, select *Site to Site*.
    - iii. For *Remote Device Type*, select *FortiGate*.
    - iv. For *NAT Configuration*, set *No NAT between sites*.
    - v. Click *Next*.
  - b. Configure the following settings for *Authentication*:
    - i. For *Remote Device*, select *IP Address*.
    - ii. In the *IP address* field, enter *172.16.200.1*.
    - iii. For *Outgoing Interface*, select *port13*.
    - iv. For *Authentication Method*, select *Pre-shared Key*.
    - v. In the *Pre-shared Key* field, enter an example key.
    - vi. Click *Next*.
  - c. Configure the following settings for *Policy & Routing*:
    - i. From the *Local Interface* dropdown menu, select the desired local interface. In this example, it is *port9*.
    - ii. Configure the *Local Subnets* as *172.16.101.0*.
    - iii. Configure the *Remote Subnets* as *10.1.100.0*.
    - iv. Click *Create*.

**To configure IPsec VPN in an HA environment using the CLI:**

1. Configure HA. In this example, two FortiGates work in active-passive mode. The HA heartbeat interfaces are WAN1 and WAN2:

```
config system ha
```

```

set group-name "FGT-HA"
set mode a-p
set password sample
set hbdev "wan1" 50 "wan2" 50
set session-pickup enable
set priority 200
set override-wait-time 10
end

```

2. Configure the WAN interface and default route. The WAN interface is the interface connected to the ISP. It can work in static mode (as shown in this example), DHCP, or PPPoE mode. The IPsec tunnel is established over the WAN interface.

- a. Configure HQ1:

```

config system interface
 edit "port1"
 set vdom "root"
 set ip 172.16.200.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 172.16.200.3
 set device "port1"
 next
end

```

- b. Configure HQ2:

```

config system interface
 edit "port25"
 set vdom "root"
 set ip 172.16.202.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 172.16.202.2
 set device "port25"
 next
end

```

3. Configure the internal (protected subnet) interface. The internal interface connects to the corporate internal network. Traffic from this interface routes out the IPsec VPN tunnel.

- a. Configure HQ1:

```

config system interface
 edit "dmz"
 set vdom "root"
 set ip 10.1.100.1 255.255.255.0
 next
end

```

- b. Configure HQ2:

```

config system interface
 edit "port9"
 set vdom "root"
 set ip 172.16.101.1 255.255.255.0
 next
end

```

4. Configure the IPsec phase1-interface. This example uses PSK as the authentication method. You can also use signature authentication.



**a. Configure HQ1:**

```
config vpn ipsec phase1-interface
 edit "to_HQ2"
 set interface "port1"
 set peertype any
 set net-device enable
 set ha-sync-esp-seqno enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.16.202.1
 set psksecret sample
 next
end
```

**b. Configure HQ2:**

```
config vpn ipsec phase1-interface
 edit "to_HQ1"
 set interface "port25"
 set peertype any
 set net-device enable
 set ha-sync-esp-seqno enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.16.200.1
 set psksecret sample
 next
end
```

**5. Configure the IPsec phase2-interface:****a. Configure HQ1:**

```
config vpn ipsec phase2-interface
 edit "to_HQ2"
 set phase1name "to_HQ2"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 set auto-negotiate enable
 next
end
```

**b. Configure HQ2:**

```
config vpn ipsec phase2-interface
 edit "to_HQ1"
 set phase1name "to_HQ1"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 set auto-negotiate enable
 next
end
```

**6. Configure static routes. Two static routes are added to reach the remote protected subnet. The blackhole route is important to ensure IPsec traffic does not match the default route when the IPsec tunnel is down.****a. Configure HQ1:**

```
config router static
 edit 2
 set dst 172.16.101.0 255.255.255.0
 set device "to_HQ2"
 next
 edit 3
 set dst 172.16.101.0 255.255.255.0
 set blackhole enable
 set distance 254
 next
end
```

```
end
```

**b. Configure HQ2:**

```
config router static
 edit 2
 set dst 10.1.100.0 255.255.255.0
 set device "to_HQ1"
 next
 edit 3
 set dst 10.1.100.0 255.255.255.0
 set blackhole enable
 set distance 254
 next
end
```

**7. Configure two firewall policies to allow bi-directional IPsec traffic flow over the IPsec tunnel:**

**a. Configure HQ1:**

```
config firewall policy
 edit 1
 set name "inbound"
 set srcintf "to_HQ2"
 set dstintf "dmz"
 set srcaddr "172.16.101.0"
 set dstaddr "10.1.100.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set name "outbound"
 set srcintf "dmz"
 set dstintf "to_HQ2"
 set srcaddr "10.1.100.0"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end
```

**b. Configure HQ2:**

```
config firewall policy
 edit 1
 set name "inbound"
 set srcintf "to_HQ1"
 set dstintf "port9"
 set srcaddr "10.1.100.0"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set name "outbound"
 set srcintf "port9"
 set dstintf "to_HQ1"
 set srcaddr "172.16.101.0"
 set dstaddr "10.1.100.0"
 set action accept
```

```

 set schedule "always"
 set service "ALL"
 next
end

```

8. Use the following diagnose commands to check IPsec phase1/phase2 interface status including the sequence number on the secondary FortiGate. The diagnose debug application ike -1 command is the key to troubleshoot why the IPsec tunnel failed to establish.

- a. Run the HQ1 # diagnose vpn ike gateway list command. The system should return the following:

```

vd: root/0
name: to_HQ2
version: 1
interface: port1 11
addr: 172.16.200.1:500 -> 172.16.202.1:500
created: 5s ago
IKE SA: created 1/1 established 1/1 time 0/0/0 ms
IPsec SA: created 2/2 established 2/2 time 0/0/0 ms
 id/spi: 12 6e8d0532e7fe8d84/3694ac323138a024 direction: responder status:
 established 5-5s ago = 0ms proposal: aes128-sha256 key: b3efb46d0d385aff-
 7bb9ee241362ee8d lifetime/rekey: 86400/86124 DPD sent/recvd: 00000000/00000000

```

- b. Run the HQ1 # diagnose vpn tunnel list command. The system should return the following:

```
list all ipsec tunnel in vd 0
```

```

name=to_HQ2 ver=1 serial=1 172.16.200.1:0->172.16.202.1:0
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_
 dev frag-rfc accept_traffic=1
proxyid_num=1 child_num=0 refcnt=11 ilast=7 olast=87 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=to_HQ2 proto=0 sa=1 ref=2 serial=1 auto-negotiate
 src: 0:0.0.0.0/0.0.0.0:0 dst: 0:0.0.0.0/0.0.0.0:0 SA: ref=3 options=18227 type=00
 soft=0 mtu=1438 expire=42927/0B replaywin=2048
 seqno=1 esn=0 replaywin_lastseq=00000000 itn=0
 life: type=01 bytes=0/0 timeout=42930/43200 dec: spi=ef9ca700 esp=aes key=16
 a2c6584bf654d4f956497b3436f1cfc7
 ah=sha1 key=20 82c5e734bce81e6f18418328e2a11aeb7baa021b
 enc: spi=791e898e esp=aes key=16 0dbb4588ba2665c6962491e85a4a8d5a
 ah=sha1 key=20 2054b318d2568a8b12119120f20ecac97ab730b3
 dec:pkts/bytes=0/0, enc:pkts/bytes=0/0

```

ESP seqno synced to primary FortiGate every five minutes, and big gap between primary and secondary to ensure that no packet is dropped after HA failover caused by tcp-replay. Check ESP sequence number synced on secondary FortiGate.

- c. Run the HQ1 # execute ha manage 0 admin command.

- d. Run the HQ1-Secondary # diagnose vpn tunnel list command. The system should return the following:

```
list all ipsec tunnel in vd 0
```

```

name=to_HQ2 ver=1 serial=1 172.16.200.1:0->172.16.202.1:0
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_
 dev frag-rfc accept_traffic=1
proxyid_num=1 child_num=0 refcnt=11 ilast=13 olast=274 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=to_HQ2 proto=0 sa=1 ref=2 serial=1 auto-negotiate

```

```
src: 0:0.0.0.0/0.0.0.0:0 dst: 0:0.0.0.0/0.0.0.0:0 SA: ref=3 options=27 type=00
soft=0 mtu=1280 expire=42740/0B replaywin=2048
seqno=47868c01 esn=0 replaywin_lastseq=00000000 itn=0
life: type=01 bytes=0/0 timeout=42930/43200 dec: spi=ef9ca700 esp=aes key=16
a2c6584bf654d4f956497b3436f1cfc7
ah=sha1 key=20 82c5e734bce81e6f18418328e2a11aeb7baa021b
enc: spi=791e898e esp=aes key=16 0dbb4588ba2665c6962491e85a4a8d5a
ah=sha1 key=20 2054b318d2568a8b12119120f20ecac97ab730b3
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

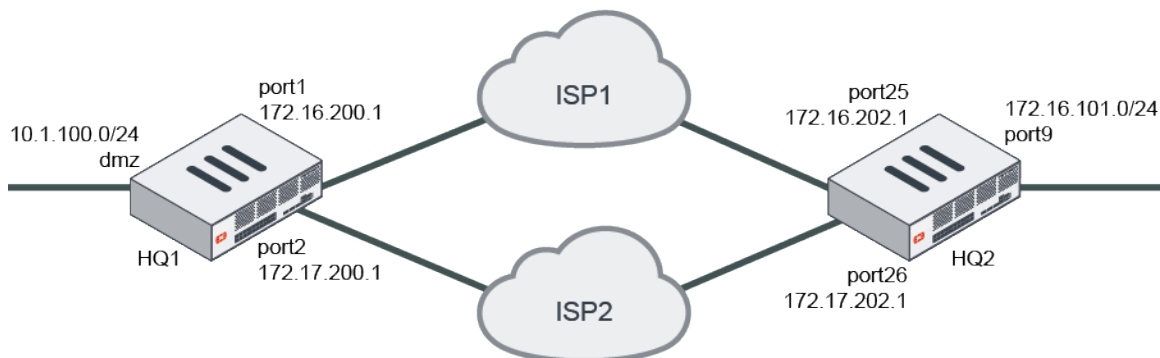
## IPsec aggregate for redundancy and traffic load-balancing

This is a sample configuration of a multiple site-to-site IPsec VPN that uses an IPsec aggregate interface to set up redundancy and traffic load-balancing. The VPN tunnel interfaces must have `net-device` disabled in order to be members of the IPsec aggregate.

Each FortiGate has two WAN interfaces connected to different ISPs. OSPF runs over the IPsec aggregate in this configuration.

The supported load balancing algorithms are: L3, L4, round-robin (default), and redundant. The first three options allow traffic to be load-balanced, while the last option (redundant) uses the first tunnel that is up for all traffic.

Dynamic routing can run on the aggregate interface, and it can be a member interface in SD-WAN (not shown in this configuration).



## Configuring the HQ1 FortiGate in the GUI

There are five steps to configure the FortiGate:

1. [Create the IPsec tunnels.](#)
2. [Create the IPsec aggregate.](#)
3. [Configure the firewall policies.](#)
4. [Configure the aggregate VPN interface IPs.](#)
5. [Configure OSPF.](#)

### To create the IPsec tunnels:

1. Go to *VPN > IPsec Wizard* and select the *Custom* template.
2. For *Name*, enter `pri_HQ2` and click *Next*.

**3. Enter the following:**

Phase 1	
IP Address	172.16.202.1
Interface	port1
Device creation	Disabled
Aggregate member	Enabled
Authentication Method	Pre-shared Key
Pre-shared Key	Enter the secure key
IKE Mode	Aggressive
Peer Options Accept Types	Any peer ID
Phase 2	
Auto-negotiate	Enable

**4. Configure the other settings as needed.****5. Click OK.****6. Create another tunnel named sec\_HQ2 with the following settings:**

Phase 1	
IP Address	172.17.202.1
Interface	port2
Device creation	Disabled
Aggregate member	Enabled
Authentication Method	Pre-shared Key
Pre-shared Key	Enter the secure key
IKE Mode	Aggressive
Peer Options Accept Types	Any peer ID
Phase 2	
Auto-negotiate	Enable

**To create the IPsec aggregate:**

1. Go to **VPN > IPsec Tunnels** and click **Create New > IPsec Aggregate**.
2. For **Name**, enter `agg_HQ2`.
3. Select a load balancing algorithm.
4. From the **Tunnel** dropdown, select the tunnels that you created previously (*pri\_HQ2* and *sec\_HQ2*). If required, enter weights for each tunnel.
5. Click **OK**.

**To configure the firewall policies:**

1. Go to *Policy & Objects > Firewall Policy*.
2. Create an inbound traffic policy with the following settings:

Name	inbound
Incoming Interface	agg_HQ2
Outgoing Interface	dmz
Source	172.16.101.0
Destination	10.1.100.0
Schedule	always
Action	ACCEPT
Service	ALL

3. Click *OK*.
4. Create an outbound traffic policy with the following settings:

Name	outbound
Incoming Interface	dmz
Outgoing Interface	agg_HQ2
Source	10.1.100.0
Destination	172.16.101.0
Schedule	always
Action	ACCEPT
Service	ALL

**To configure the aggregate VPN interface IPs:**

1. Go to *Network > Interfaces* and edit *agg\_HQ2*.
2. For *IP*, enter 10.10.10.1.
3. For *Remote IP/Netmask*, enter 10.10.10.2 255.255.255.255.
4. Click *OK*.

**To configure OSPF:**

1. Go to *Network > OSPF*.
2. For *Router ID*, enter 1.1.1.1.
3. In the *Areas* table, click *Create New*.
  - a. For *Area ID*, enter 0.0.0.0.
  - b. Click *OK*.

4. In the *Networks* table, click *Create New*.
  - a. Set the *Area* to *0.0.0.0*.
  - b. For *IP/Netmask*, enter *10.1.100.0/24*.
  - c. Click *OK*.
  - d. Click *Create New*.
  - e. For *IP/Netmask*, enter *10.10.10.0/24*.
  - f. Click *OK*.
5. Click *Apply*.

## Configuring the HQ2 FortiGate in the GUI

There are five steps to configure the FortiGate:

1. [Create the IPsec tunnels](#).
2. [Create the IPsec aggregate](#).
3. [Configure the firewall policies](#).
4. [Configure the aggregate VPN interface IPs](#).
5. [Configure OSPF](#).

### To create the IPsec tunnels:

1. Go to *VPN > IPsec Wizard* and select the *Custom* template.
2. For *Name*, enter *pri\_HQ1* and click *Next*.
3. Enter the following:

#### Phase 1

IP Address	172.16.200.1
Interface	port25
Device creation	Disabled
Aggregate member	Enabled
Authentication Method	Pre-shared Key
Pre-shared Key	Enter the secure key
IKE Mode	Aggressive
Peer Options Accept Types	Any peer ID

#### Phase 2

Auto-negotiate	Enable
----------------	--------

4. Configure the other settings as needed.
5. Click *OK*.
6. Create another tunnel named *sec\_HQ1* with the following settings:

#### Phase 1

IP Address	172.17.200.1
------------	--------------

Interface	port26
Device creation	Disabled
Aggregate member	Enabled
Authentication Method	Pre-shared Key
Pre-shared Key	Enter the secure key
IKE Mode	Aggressive
Peer Options Accept Types	Any peer ID
<b>Phase 2</b>	
Auto-negotiate	Enable

### To create the IPsec aggregate:

1. Go to *VPN > IPsec Tunnels* and click *Create New > IPsec Aggregate*.
2. For *Name*, enter `agg_HQ1`.
3. Select a load balancing algorithm.
4. From the *Tunnel* dropdown, select the tunnels that you created previously (*pri\_HQ1* and *sec\_HQ1*). If required, enter weights for each tunnel.
5. Click *OK*.

### To configure the firewall policies:

1. Go to *Policy & Objects > Firewall Policy*.
2. Create an inbound traffic policy with the following settings:

Name	inbound
Incoming Interface	agg_HQ1
Outgoing Interface	port9
Source	10.1.100.0
Destination	172.16.101.0
Schedule	always
Action	ACCEPT
Service	ALL

3. Click *OK*.
4. Create an outbound traffic policy with the following settings:

Name	outbound
Incoming Interface	port9
Outgoing Interface	agg_HQ1



Source	172.16.101.0
Destination	10.1.100.0
Schedule	always
Action	ACCEPT
Service	ALL

### To configure the aggregate VPN interface IPs:

1. Go to *Network > Interfaces* and edit *agg\_HQ1*.
2. For *IP*, enter 10.10.10.2.
3. For *Remote IP/Netmask*, enter 10.10.10.1 255.255.255.255.
4. Click *OK*.

### To configure OSPF:

1. Go to *Network > OSPF*.
2. For *Router ID*, enter 2.2.2.2.
3. In the *Areas* table, click *Create New*.
  - a. For *Area ID*, enter 0.0.0.0.
  - b. Click *OK*.
4. In the *Networks* table, click *Create New*.
  - a. Set the *Area* to 0.0.0.0.
  - b. For *IP/Netmask*, enter 172.16.101.0/24.
  - c. Click *OK*.
  - d. Click *Create New*.
  - e. For *IP/Netmask*, enter 10.10.10.0/24.
  - f. Click *OK*.
5. Click *Apply*.

## Monitoring the traffic in the GUI

### To monitor the traffic:

1. Go to *Dashboard > Network*, hover over the *IPsec* widget, then click *Expand to Full Screen*.
2. Expand the aggregate tunnel in the table to view statistics for each aggregate member.

## Configuring the HQ1 FortiGate in the CLI

There are six steps to configure the FortiGate:

1. [Configure the interfaces.](#)
2. [Configure two IPsec phase 1 and phase 2 interfaces.](#)
3. [Configure the IPsec aggregate.](#)
4. [Configure the firewall policies.](#)
5. [Configure the aggregate VPN interface IPs.](#)
6. [Configure OSPF.](#)

**To configure the interfaces:**

1. Configure port1, port2, and dmz as shown in the topology diagram.

**To configure two IPsec phase 1 and phase 2 interfaces:**

```
config vpn ipsec phase1-interface
 edit "pri_HQ2"
 set interface "port1"
 set peertype any
 set net-device disable
 set aggregate-member enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.16.202.1
 set psksecret sample1
 next
 edit "sec_HQ2"
 set interface "port2"
 set peertype any
 set net-device disable
 set aggregate-member enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.17.202.1
 set psksecret sample2
 next
end
config vpn ipsec phase2-interface
 edit "pri_HQ2"
 set phase1name "pri_HQ2"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
 chacha20poly1305
 set auto-negotiate enable
 next
 edit "sec_HQ2"
 set phase1name "sec_HQ2"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
 chacha20poly1305
 set auto-negotiate enable
 next
end
```

**To configure the IPsec aggregate:**

```
config system ipsec-aggregate
 edit "agg_HQ2"
 set member "pri_HQ2" "sec_HQ2"
 next
end
```

**To configure the firewall policies:**

```
config firewall policy
 edit 1
 set name "inbound"
 set srcintf "agg_HQ2"
 set dstintf "dmz"
```

```
 set srcaddr "172.16.101.0"
 set dstaddr "10.1.100.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set name "outbound"
 set srcintf "dmz"
 set dstintf "agg_HQ2"
 set srcaddr "10.1.100.0"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end
```

### To configure the aggregate VPN interface IPs:

```
config system interface
 edit "agg_HQ2"
 set ip 10.10.10.1 255.255.255.255
 set remote-ip 10.10.10.2 255.255.255.255
 next
end
```

### To configure OSPF:

```
config router ospf
 set router-id 1.1.1.1
 config area
 edit 0.0.0.0
 next
 end
 config network
 edit 1
 set prefix 10.1.100.0 255.255.255.0
 next
 edit 2
 set prefix 10.10.10.0 255.255.255.0
 next
 end
end
```

## Configuring the HQ2 FortiGate in the CLI

There are six steps to configure the FortiGate:

1. [Configure the interfaces.](#)
2. [Configure two IPsec phase 1 and phase 2 interfaces.](#)
3. [Configure the IPsec aggregate.](#)
4. [Configure the firewall policies.](#)
5. [Configure the aggregate VPN interface IPs.](#)
6. [Configure OSPF.](#)

**To configure the interfaces:**

1. Configure port25, port26, and port9 as shown in the topology diagram.

**To configure two IPsec phase 1 and phase 2 interfaces:**

```
config vpn ipsec phase1-interface
 edit "pri_HQ1"
 set interface "port25"
 set peertype any
 set net-device disable
 set aggregate-member enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.16.200.1
 set psksecret sample1
 next
 edit "sec_HQ1"
 set interface "port26"
 set peertype any
 set net-device disable
 set aggregate-member enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.17.200.1
 set psksecret sample2
 next
end
config vpn ipsec phase2-interface
 edit "pri_HQ1"
 set phase1name "pri_HQ1"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
 chacha20poly1305
 set auto-negotiate enable
 next
 edit "sec_HQ1"
 set phase1name "sec_HQ1"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm
 chacha20poly1305
 set auto-negotiate enable
 next
end
```

**To configure the IPsec aggregate:**

```
config system ipsec-aggregate
 edit "agg_HQ1"
 set member "pri_HQ1" "sec_HQ1"
 next
end
```

**To configure the firewall policies:**

```
config firewall policy
 edit 1
 set name "inbound"
 set srcintf "agg_HQ1"
 set dstintf "port9"
```

```
 set srcaddr "10.1.100.0"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set name "outbound"
 set srcintf "port9"
 set dstintf "agg_HQ1"
 set srcaddr "172.16.101.0"
 set dstaddr "10.1.100.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end
```

### To configure the aggregate VPN interface IPs:

```
config system interface
 edit "agg_HQ1"
 set ip 10.10.10.2 255.255.255.255
 set remote-ip 10.10.10.1 255.255.255.255
 next
end
```

### To configure OSPF:

```
config router ospf
 set router-id 2.2.2.2
 config area
 edit 0.0.0.0
 next
 end
 config network
 edit 1
 set prefix 172.16.101.0 255.255.255.0
 next
 edit 2
 set prefix 10.10.10.0 255.255.255.0
 next
 end
end
```

## Monitoring the traffic in the CLI

### To view debugging information:

1. Verify the status of the phase 1 IKE SAs:  
# diagnose vpn ike gateway list  
vd: root/0  
name: pri\_HQ2  
version: 1  
interface: port1 11

```

addr: 172.16.200.1:500 -> 172.16.202.1:500
created: 1520s ago
IKE SA: created 1/2 established 1/1 time 10/10/10 ms
IPsec SA: created 2/2 established 1/1 time 0/0/0 ms
 id/spi: 173 dcdede154681579b/e32f4c48c4349fc0 direction: responder status: established
 1498-1498s ago = 10ms proposal: aes128-sha256 key: d7230a68d7b83def-
 588b94495cfa9d38 lifetime/rekey: 86400/84631 DPD sent/recvd: 0000000d/00000006
vd: root/0
name: sec_HQ2
version: 1
interface: port2 12
addr: 172.17.200.1:500 -> 172.17.202.1:500
created: 1520s ago
IKE SA: created 1/2 established 1/1 time 10/10/10 ms
IPsec SA: created 2/2 established 1/1 time 0/0/0 ms
 id/spi: 174 a567bd7bf02a04b5/4251b6254660aee2 direction: responder status: established
 1498-1498s ago = 10ms proposal: aes128-sha256 key: 9f44f500c28d8de6-
 febaae9d1e6a164c lifetime/rekey: 86400/84631 DPD sent/recvd: 00000008/0000000c

```

## 2. Verify the phase 2 IPsec tunnel SAs:

```

diagnose vpn tunnel list
list all ipsec tunnel in vd 0
name=sec_HQ2 ver=1 serial=2 172.17.200.1:0->172.17.202.1:0
bound_if=5 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/512 options[0200]=frag-rfc
 run_state=1 accept_traffic=1
proxyid_num=1 child_num=0 refcnt=7 ilast=5 olast=5 ad=/0
stat: rxp=39 txp=40 rxb=5448 txb=2732
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=15
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=sec_HQ2 proto=0 sa=1 ref=2 serial=2 auto-negotiate
 src: 0:0.0.0.0/0.0.0.0:0 dst: 0:0.0.0.0/0.0.0.0:0 SA: ref=3 options=18227 type=00
 soft=0 mtu=1438 expire=41230/0B replaywin=2048
 seqno=29 esn=0 replaywin_lastseq=00000028 itn=0
 life: type=01 bytes=0/0 timeout=42899/43200 dec: spi=1071b4f9 esp=aes key=16
 1f4dbb78bea8e97650b52d8170b5ece7
 ah=sha1 key=20 cd9bf2de0f49296cf489dd915d7baf6d78bc8f12
 enc: spi=ec89b7ee esp=aes key=16 0546efecd0d1b9ba5944f635896e4404
 ah=sha1 key=20 34599bc7dc25e1ce63ac9615bd50928ce0667dc8
 dec:pkts/bytes=39/2796, enc:pkts/bytes=40/5456
name=pri_HQ2 ver=1 serial=1 172.16.200.1:0->172.16.202.1:0
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/512 options[0200]=frag-rfc
 run_state=1 accept_traffic=1
proxyid_num=1 child_num=0 refcnt=5 ilast=15 olast=15 ad=/0
stat: rxp=38 txp=39 rxb=5152 txb=2768
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=20
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=pri_HQ2 proto=0 sa=1 ref=2 serial=2 auto-negotiate
 src: 0:0.0.0.0/0.0.0.0:0 dst: 0:0.0.0.0/0.0.0.0:0 SA: ref=3 options=18227 type=00
 soft=0 mtu=1438 expire=41231/0B replaywin=2048
 seqno=28 esn=0 replaywin_lastseq=00000027 itn=0
 life: type=01 bytes=0/0 timeout=42900/43200 dec: spi=1071b4f8 esp=aes key=16
 142cce377b3432ba41e64128ade6848c
 ah=sha1 key=20 20e64947e2397123f561584321adc0e7aa0c342d
 enc: spi=ec89b7ed esp=aes key=16 2ec13622fd60dacce3d28ebe5fe7ab14
 ah=sha1 key=20 c1787497508a87f40c73c0db0e835c70b3c3f42d
 dec:pkts/bytes=38/2568, enc:pkts/bytes=39/5432

```

## 3. Debug the IPsec aggregation list:

```
diagnose sys ipsec-aggregate list
```

```

agg_HQ2 algo=RR member=2 run_tally=2
members:
 pri_HQ2
 sec_HQ2

```

#### 4. Verify the OSPF neighbor information:

```

get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID Pri State Dead Time Address Interface
2.2.2.2 1. Full/ - 00:00:34 10.10.10.2 agg1_HQ2

```

#### 5. Verify the OSPF routing table:

```

get router info routing-table ospf
Routing table for VRF=0
O 172.16.101.0/24 [110/20] via 10.10.10.2, agg1_HQ2 , 00:18:43

```

## Per packet distribution and tunnel aggregation

This example shows how to aggregate IPsec tunnels by using per-packet load-balancing among IPsec tunnels.

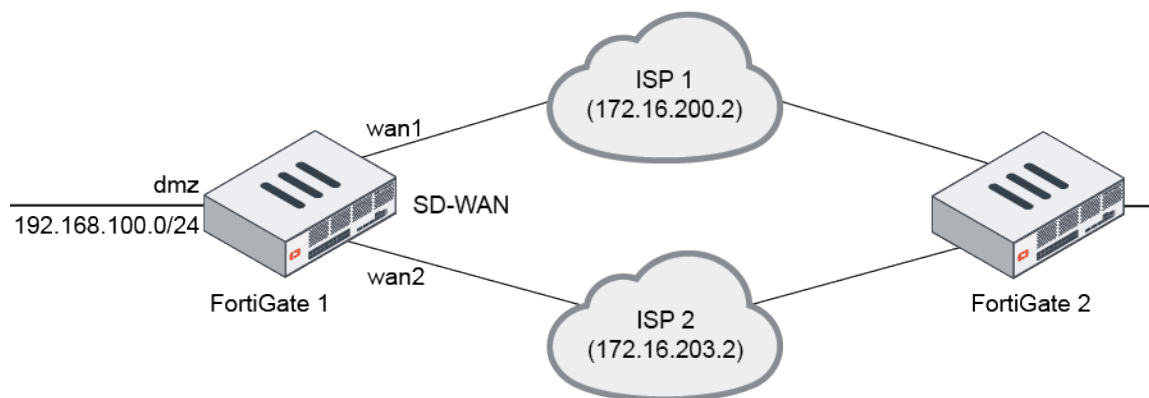
For example, a customer has two ISP connections, wan1 and wan2. Using these two connections, we create two VPN interfaces and configure traffic for per-packet load-balancing among IPsec tunnels.



This feature only allows static/DDNS tunnels to be members.

Dynamic (dialup) tunnels are not allowed because dialup instances tend to have different locations and hence different routing. This conflicts with the rule that all the members of an aggregate must have the same routing.

## Sample topology



## Sample configuration

On the FortiGate, first create two IPsec VPN interfaces. Then create an `ipsec-aggregate` interface and add this interface as an SD-WAN member.

## FortiGate 1 configuration

### To create two IPsec VPN interfaces on FortiGate 1:

```
config vpn ipsec phase1-interface
 edit "vd1-p1"
 set interface "wan1"
 set peertype any
 set net-device disable
 set aggregate-member enable
 set proposal aes256-sha256
 set dhgrp 14
 set remote-gw 172.16.201.2
 set psksecret ftnt1234
 next
 edit "vd1-p2"
 set interface "wan2"
 set peertype any
 set net-device disable
 set aggregate-member enable
 set proposal aes256-sha256
 set dhgrp 14
 set remote-gw 172.16.202.2
 set psksecret ftnt1234
 next
end
config vpn ipsec phase2-interface
 edit "vd1-p1"
 set phase1name "vd1-p1"
 next
 edit "vd1-p2"
 set phase1name "vd1-p2"
 next
end
```

### To create an ipsec-aggregate interface on FortiGate 1:

```
config system ipsec-aggregate
 edit "aggl"
 set member "vd1-p1" "vd1-p2"
 set algorithm L3
 next
end
config system interface
 edit "aggl"
 set vdom "root"
 set ip 172.16.11.1 255.255.255.255
 set allowaccess ping
 set remote-ip 172.16.11.2 255.255.255.255
 next
end
```

### To configure the firewall policy on FortiGate 1:

```
config firewall policy
 edit 1
```



```
 set name "1"
 set srcintf "dmz"
 set dstintf ""virtual-wan-link""
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set nat enable
 next
end
```

### **To configure SD-WAN on FortiGate 1:**

```
config system virtual-wan-link
 set status enable
 config members
 edit 1
 set interface "aggl"
 set gateway 172.16.11.2
 next
 end
end
```

### **FortiGate 2 configuration**

#### **To create two IPsec VPN interfaces on FortiGate 2:**

```
config vpn ipsec phase1-interface
 edit "vd2-p1"
 set interface "wan1"
 set peertype any
 set net-device disable
 set proposal aes256-sha256
 set dhgrp 14
 set remote-gw 172.16.200.1
 set psksecret ftnt1234
 next
 edit "vd2-p2"
 set interface "wan2"
 set peertype any
 set net-device disable
 set proposal aes256-sha256
 set dhgrp 14
 set remote-gw 172.16.203.1
 set psksecret ftnt1234
 next
end
config vpn ipsec phase2-interface
 edit "vd2-p1"
 set phase1name "vd2-p1"
 next
 edit "vd2-p2"
 set phase1name "vd2-p2"
```

```
 next
end
```

**To create an ipsec-aggregate interface on FortiGate 2:**

```
config system ipsec-aggregate
 edit "agg2"
 set member "vd2-p1" "vd2-p2"
 set algorithm L3
 next
end
config system interface
 edit "agg2"
 set vdom "root"
 set ip 172.16.11.2 255.255.255.255
 set allowaccess ping
 set remote-ip 172.16.11.1 255.255.255.255
 next
end
```

**To configure the firewall policy on FortiGate 2:**

```
config firewall policy
 edit 1
 set name "1"
 set srcintf "dmz"
 set dstintf ""virtual-wan-link""
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set nat enable
 next
end
```

**To configure SD-WAN on FortiGate 2:**

```
config system virtual-wan-link
 set status enable
 config members
 edit 1
 set interface "agg2"
 set gateway 172.16.11.1
 next
 end
end
```

**To use the diagnose command to display aggregate IPsec members:**

```
diagnose sys ipsec-aggregate list
agg1 algo=L3 member=2 run_tally=2
members:
 vd1-p1
 vd1-p2
```

**To use the diagnose command to check VPN status:**

```
diagnose vpn tunnel list
list all ipsec tunnel in vd 0

name=vd1-p1 ver=1 serial=2 172.16.200.1:0->172.16.201.2:0 dst_mtu=0
bound_if=10 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/520 options[0208]=npu frag-rfc
run_state=1 accept_traffic=0

proxyid_num=1 child_num=0 refcnt=5 ilast=15 olast=676 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=vd1-p1 proto=0 sa=0 ref=1 serial=1
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0

name=vd1-p2 ver=1 serial=3 172.16.203.1:0->172.16.202.2:0 dst_mtu=1500
bound_if=28 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/520 options[0208]=npu frag-rfc
run_state=1 accept_traffic=1

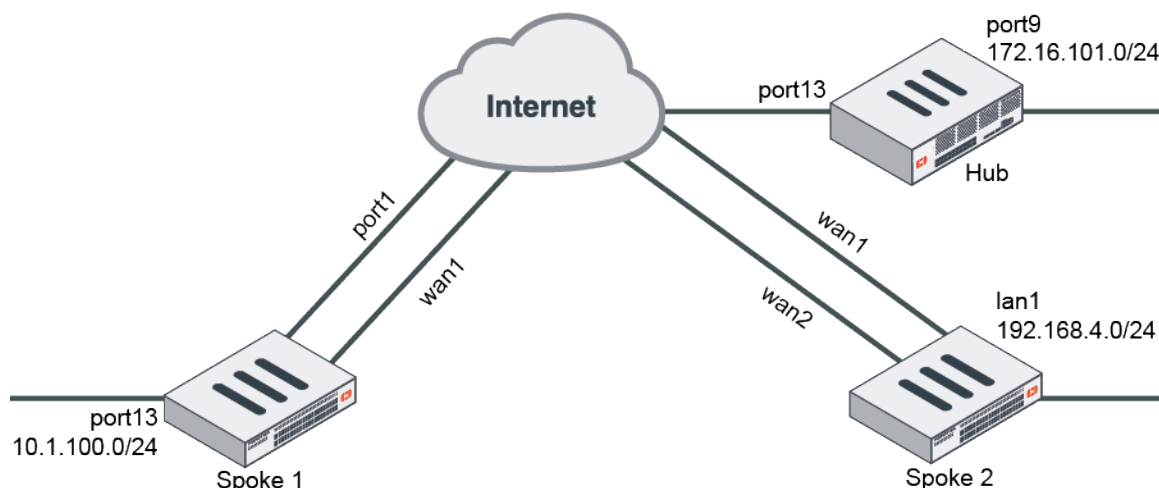
proxyid_num=1 child_num=0 refcnt=12 ilast=1 olast=1 ad=/0
stat: rxp=1 txp=1686 rxb=16602 txb=111717
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=vd1-p2 proto=0 sa=1 ref=9 serial=1
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0
 SA: ref=4 options=10226 type=00 soft=0 mtu=1438 expire=42164/0B replaywin=2048
 seqno=697 esn=0 replaywin_lastseq=00000002 itn=0 qat=0
 life: type=01 bytes=0/0 timeout=42902/43200
 dec: spi=f6ae9f83 esp=aes key=16 f6855c72295e3c5c49646530e6b96002
 ah=sha1 key=20 f983430d6c161d0a4cd9007c7ae057f1ff011334
 enc: spi=8c72bala esp=aes key=16 6330f8c532a6ca5c5765f6a9a6034427
 ah=sha1 key=20 e5fe385ed5f0f6a33f1d507601b15743a8c70187
 dec:pkts/bytes=1/16536, enc:pkts/bytes=1686/223872
 npu_flag=02 npu_rgwy=172.16.202.2 npu_lgwy=172.16.203.1 npu_selid=2 dec_npuid=1 enc_
 npuid=0
```

**Redundant hub and spoke VPN**

A redundant hub and spoke configuration allows VPN connections to radiate from a central FortiGate unit (the hub) to multiple remote peers (the spokes). Traffic can pass between private networks behind the hub and private networks behind the remote peers. Traffic can also pass between remote peer private networks through the hub.

This is a sample configuration of hub and spoke IPsec VPN. The following applies for this scenario:

- The spokes have two WAN interfaces and two IPsec VPN tunnels for redundancy.
- The secondary VPN tunnel is up only when the primary tunnel is down by dead peer detection.



Because the GUI can only complete part of the configuration, we recommend using the CLI.

### To configure redundant hub and spoke VPN using the FortiOS CLI:

#### 1. Configure the hub.

##### a. Configure the WAN, internal interface, and static route.

```

config system interface
 edit "port13"
 set alias "WAN"
 set ip 172.16.202.1 255.255.255.0
 next
 edit "port9"
 set alias "Internal"
 set ip 172.16.101.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 172.16.202.2
 set device "port13"
 next
end

```

##### b. Configure the IPsec phase1-interface and phase2-interface.

```

config vpn ipsec phase1-interface
 edit "hub"
 set type dynamic
 set interface "port13"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set dpd on-idle
 set psksecret sample
 set dpd-retryinterval 60
 next
end
config vpn ipsec phase2-interface
 edit "hub"
 set phase1name "hub"
 next
end

```

```
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 next
end
```

**c. Configure the firewall policy.**

```
config firewall policy
 edit 1
 set name "spoke-hub"
 set srcintf "hub"
 set dstintf "port9"
 set srcaddr "all"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set name "spoke-spoke"
 set srcintf "hub"
 set dstintf "hub"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end
```

**2. Configure the spokes.**

**a. Configure the WAN, internal interface, and static route.**

**i. Configure Spoke1.**

```
config system interface
 edit "port1"
 set ip 172.16.200.1 255.255.255.0
 next
 edit "wan1"
 set mode dhcp
 set distance 10
 set priority 100
 next
 edit "dmz"
 set ip 10.1.100.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 172.16.200.2
 set device "port1"
 next
end
```

**ii. Configure Spoke2.**

```
config system interface
 edit "wan1"
 set ip 172.16.200.3 255.255.255.0
 next
 edit "wan2"
 set mode dhcp
```

```

 set distance 10
 set priority 100
 next
 edit "lan1"
 set ip 192.168.4.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 172.16.200.2
 set device "wan1"
 next
end

```

**b. Configure IPsec phase1-interface and phase2-interface.**

**i. Configure Spoke1.**

```

config vpn ipsec phase1-interface
 edit "primary"
 set interface "port1"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.16.202.1
 set psksecret sample
 next
 edit "secondary"
 set interface "wan1"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.16.202.1
 set monitor "primary"
 set psksecret sample
 next
end
config vpn ipsec phase2-interface
 edit "primary"
 set phasename "primary"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 set auto-negotiate enable
 set src-subnet 10.1.100.0 255.255.255.0
 next
 edit "secondary"
 set phasename "secondary"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 set auto-negotiate enable
 set src-subnet 10.1.100.0 255.255.255.0
 next
end

```

**ii. Configure Spoke2.**

```

config vpn ipsec phase1-interface
 edit "primary"
 set interface "wan1"
 set peertype any
 set net-device enable

```

```

 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.16.202.1
 set psksecret sample
 next
 edit "secondary"
 set interface "wan2"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set remote-gw 172.16.202.1
 set monitor "primary"
 set psksecret sample
 next
end
config vpn ipsec phase2-interface
 edit "primary"
 set phasename "primary"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 set auto-negotiate enable
 set src-subnet 192.168.4.0 255.255.255.0
 next
 edit "secondary"
 set phasename "secondary"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 set auto-negotiate enable
 set src-subnet 192.168.4.0 255.255.255.0
 next
end

```

**c. Configure the firewall policy.**

**i. Configure Spoke1.**

```

config firewall policy
 edit 1
 set srcintf "dmz"
 set dstintf "primary" "secondary"
 set srcaddr "10.1.100.0"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end

```

**ii. Configure Spoke2.**

```

config firewall policy
 edit 1
 set srcintf "lan1"
 set dstintf "primary" "secondary"
 set srcaddr "192.168.4.0"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end

```

**d. Configure the static route.****i. Configure Spoke1.**

```

config router static
edit 3
set dst 172.16.101.0 255.255.255.0
set distance 1
set device "primary"
next
edit 4
set dst 172.16.101.0 255.255.255.0
set distance 3
set device "secondary"
next
end

```

**ii. Configure Spoke2.**

```

config router static
edit 3
set dst 172.16.101.0 255.255.255.0
set distance 1
set device "primary"
next
edit 4
set dst 172.16.101.0 255.255.255.0
set distance 3
set device "secondary"
next
end

```

**3. Run diagnose and get commands.****a. Run the Spoke1 # diagnose vpn tunnel list command. The system should return the following:**

```

name=primary ver=1 serial=1 172.16.200.1:0->172.16.202.1:0
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_
dev frag-rfc accept_traffic=1
proxyid_num=1 child_num=0 refcnt=15 ilast=0 olast=0 ad=/0
stat: rxp=1879 txp=1881 rxb=225480 txb=112860
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=primary proto=0 sa=1 ref=2 serial=2 auto-negotiate
src: 0:10.1.100.0/255.255.255.0:0 dst: 0:0.0.0.0/0.0.0.0:0 SA: ref=3 options=18227
type=00 soft=0 mtu=1438 expire=41002/0B replaywin=2048
seqno=758 esn=0 replaywin_lastseq=00000758 itn=0
life: type=01 bytes=0/0 timeout=42901/43200 dec: spi=0908732f esp=aes key=16
20770dfe67ea22dd8ec32c44d84ef4d5
ah=sha1 key=20 edc89fc2ec06309ba13de95e7e486f9b795b8707
enc: spi=a1d9eed1 esp=aes key=16 8eeea2526fba062e680d941083c8b5d1
ah=sha1 key=20 f0f5deaf88b2a69046c3154e9f751739b3f411f5
dec:pkts/bytes=1879/112740, enc:pkts/bytes=1879/225480
name=secondary ver=1 serial=2 172.17.200.1:0->172.16.202.1:0
bound_if=5 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_
dev frag-rfc accept_traffic=0
proxyid_num=1 child_num=0 refcnt=10 ilast=1892 olast=1892 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=secondary proto=0 sa=0 ref=2 serial=2 auto-negotiate
src: 0:10.1.100.0/255.255.255.0:0 dst: 0:0.0.0.0/0.0.0.0:0

```



- b. Run the `Spoke1 # get router info routing-table static` command. The system should return the following:

```
Routing table for VRF=0
.....
S 172.16.101.0/24 [1/0] is directly connected, primary
```

## Overlay Controller VPN (OCVPN)

Overlay Controller VPN (OCVPN) is a cloud based solution to simplify IPsec VPN setup. When OCVPN is enabled, IPsec phase1-interfaces, phase2-interfaces, static routes, and firewall policies are generated automatically on all FortiGates that belong to the same community network. A community network is defined as all FortiGates registered to FortiCare using the same FortiCare account.

If the network topology changes on any FortiGates in the community (such as changing a public IP address in DHCP mode, adding or removing protected subnets, failing over in dual WAN), the IPsec-related configuration for all devices is updated with Cloud assistance in self-learning mode. No intervention is required.



OCVPN with SD-WAN is not currently supported.

---

The following topics provide instructions on configuring OCVPN:

- [Full mesh OCVPN on page 1283](#)
- [Hub-spoke OCVPN with ADVPN shortcut on page 1287](#)
- [Hub-spoke OCVPN with inter-overlay source NAT on page 1292](#)
- [OCVPN portal on page 1296](#)
- [Troubleshooting OCVPN on page 1297](#)

## Full mesh OCVPN

This example shows how to configure a full mesh Overlay Controller VPN (OCVPN), establishing full mesh IPsec tunnels between all of the FortiGates.

### License

- Free license: Three devices full mesh, 10 overlays, 16 subnets per overlay.
- Full License: Maximum of 16 devices, 10 overlays, 16 subnets per overlay.

### Prerequisites

- All FortiGates must be running FortiOS 6.2.0 or later.
- All FortiGates must have Internet access.
- All FortiGates must be registered on FortiCare using the same FortiCare account.

### Restrictions

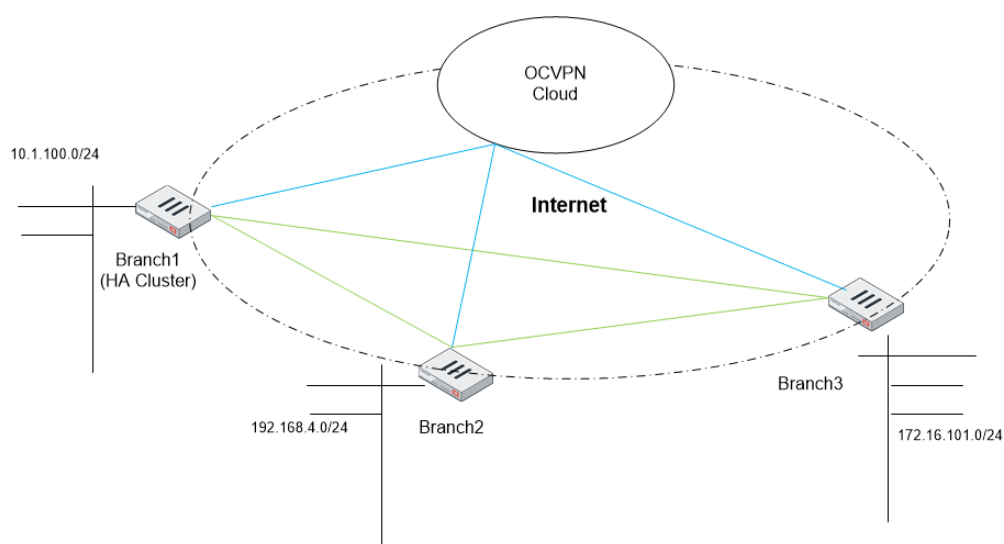
- Non-root VDOMs do not support OCVPN.
- FortiOS 6.2.x is not compatible with FortiOS 6.0.x.

## Terminology

<b>Poll-interval</b>	How often FortiGate tries to fetch OCVPN-related data from OCVPN Cloud.
<b>Role</b>	The device OCVPN role of spoke, primary-hub, or secondary-hub.
<b>Overlay</b>	Defines network overlays and bind to subnets.
<b>Subnet</b>	Internal network subnet (IPsec protected subnet). Traffic to or from this subnet enters the IPsec tunnel encrypted by IPsec SA.

## Sample topology

The following example shows three FortiGate units registered on FortiCare using the same FortiCare account. Each FortiGate unit has one internal subnet, and no NAT exists between the units.



## Sample configuration

The following overlays and subnets are used:

- Branch1:
  - Overlay name: QA. Local subnets: 10.1.100.0/24
  - Overlay name: PM. Local subnets: 10.2.100.0/24
- Branch2:
  - Overlay name: QA. Local interfaces: lan1
  - Overlay name: PM. Local interfaces: lan2
- Branch3:
  - Overlay name: QA. Local subnets: 172.16.101.0/24
  - Overlay name: PM. Local subnets: 172.16.102.0/24



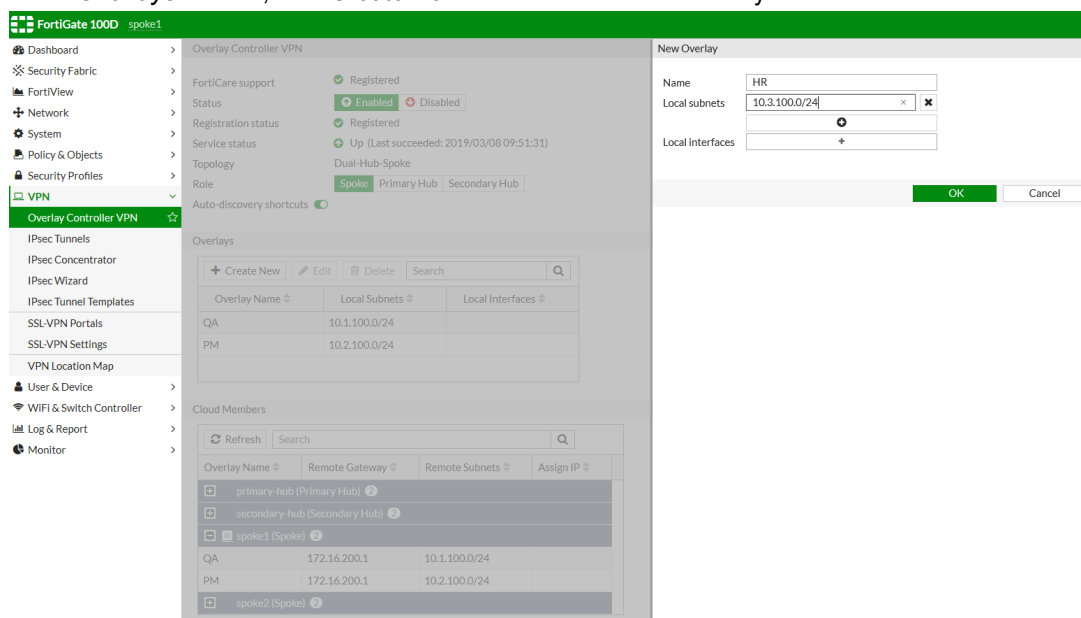
The overlay names on each device must be the same for local and remote selector pairs to be negotiated.

## To register FortiGates on FortiCare:

1. Go to *System > FortiGuard > License Information > FortiCare Support*.
2. To register, click *Register* or *Launch Portal*.
3. Complete the options to register FortiGate on FortiCare.

## To enable OCVPN using the GUI:

1. Go to *VPN > Overlay Controller VPN*.
2. Create the first overlay by setting the following options:
  - a. For *Status*, click *Enabled*.
  - b. For *Role*, click *Spoke*.
  - c. In the *Overlays* section, click *Create New* to create a network overlay.



3. Specify the *Name*, *Local subnets*, and/or *Local interfaces*.  
The local subnet must be routable and interfaces must have IP addresses.

## 4. Click OK.

FortiGate 100D branch1

Dashboard > Overlay Controller VPN

Security Fabric >

FortiView >

Network >

System >

Policy & Objects >

Security Profiles >

VPN >

Overlay Controller VPN ☆

IPsec Tunnels

IPsec Concentrator

IPsec Wizard

IPsec Tunnel Templates

SSL-VPN Portals

SSL-VPN Settings

VPN Location Map

User & Device >

WiFi & Switch Controller >

Log & Report >

Monitor >

FortiCare support Registered

Status Enabled Disabled

Registration status Registered

Service status Up (Last succeeded: 2019/03/07 16:34:00)

Topology Full-Mesh

Role Spoke Primary Hub Secondary Hub

Auto-discovery shortcuts

Overlays

+ Create New Edit Delete Search

Overlay Name	Local Subnets	Local Interfaces
QA	10.1.100.0/24	
PM	10.2.100.0/24	

Cloud Members

Refresh Search

Overlay Name	Remote Gateway	Remote Subnets
+ branch2 (Spoke) 2		
+ branch1 (Spoke) 2		
+ branch3 (Spoke) 2		

Apply

5. Click *Apply* to commit the configuration.

## 6. Repeat this procedure to create all the overlays.

## To enable OCVPN using the CLI:

## 1. Configure Branch1:

```
config vpn ocvpn
 set status enable
 config overlays
 edit 1
 set name "QA"
 config subnets
 edit 1
 set subnet 10.1.100.0 255.255.255.0
 next
 end
 next
 next
 edit 2
 set name "PM"
 config subnets
 edit 1
 set subnet 10.2.100.0 255.255.255.0
 next
 end
 next
end
```

```
 end
end
```

## 2. Configure Branch2:

```
config vpn ocvpn
 set status enable
 config overlays
 edit 1
 set name "QA"
 config subnets
 edit 1
 set type interface
 set interface "lan1"
 next
 end
 next
 edit 2
 set name "PM"
 config subnets
 edit 1
 set type interface
 set interface "lan2"
 next
 end
 next
end
end
```

## 3. Configure Branch3:

```
config vpn ocvpn
 set status enable
 config overlays
 edit 1
 set name "QA"
 config subnets
 edit 1
 set subnet 172.16.101.0 255.255.255.0
 next
 end
 next
 edit 1
 set name "PM"
 config subnets
 edit 1
 set subnet 172.16.102.0 255.255.255.0
 next
 end
 next
end
end
```

## Hub-spoke OCVPN with ADVPN shortcut

This topic shows a sample configuration of a hub-spoke One-Click VPN (OCVPN) with an Auto Discovery VPN (ADVPN) shortcut. OCVPN automatically detects the network topology based on members' information. To form a hub-spoke

OCVPN, at least one device must announce its role as the primary hub, another device can work as the secondary hub (for redundancy), while others function as spokes.

## License

- Free license: Hub-spoke network topology not supported.
- Full license: Maximum of 2 hubs, 10 overlays, 64 subnets per overlay; 512 spokes, 10 overlays, 16 subnets per overlay.

## Prerequisites

- All FortiGate must be running FortiOS 6.2.0 or later.
- All FortiGate must have Internet access.
- All FortiGate must be registered on FortiCare using the same FortiCare account.

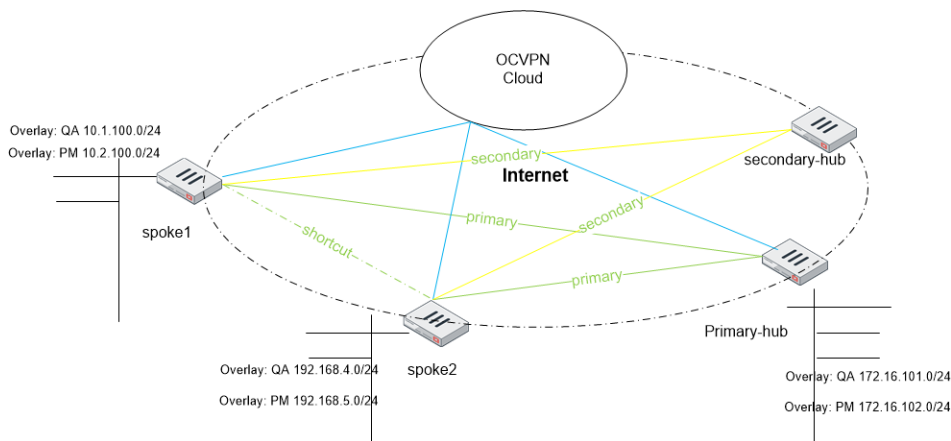
## Restrictions

- Non-root VDOMs do not support OCVPN.
- FortiOS 6.2.x is not compatible with FortiOS 6.0.x.

## OCVPN device roles

- Primary hub.
- Secondary hub.
- Spoke (OCVPN default role).

## Sample topology



## Sample configuration

The steps below use the following overlays and subnets for the sample configuration:

- Primary hub:
  - Overlay name: QA. Local subnets: 172.16.101.0/24
  - Overlay name: PM. Local subnets: 172.16.102.0/24

- Secondary hub:
  - Overlays are synced from primary hub.
- Spoke1:
  - Overlay name: QA. Local subnets: 10.1.100.0/24
  - Overlay name: PM. Local subnets: 10.2.100.0/24
- Spoke2:
  - Overlay name: QA. Local interfaces: lan1
  - Overlay name: PM. Local interfaces: lan2



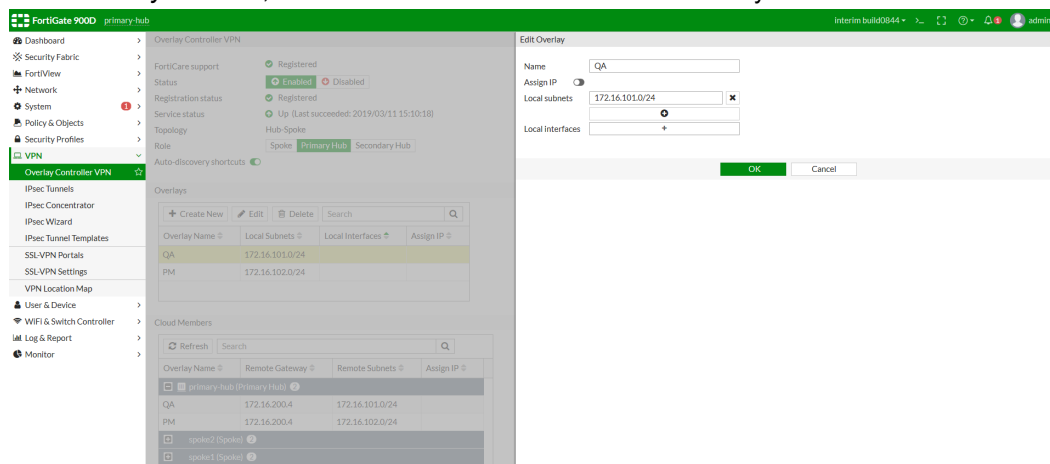
The overlay names on each device must be the same for local and remote selector pairs to be negotiated.

### To register FortiGates on FortiCare:

1. Go to *System > FortiGuard > License Information > FortiCare Support*.
2. To register, click *Register* or *Launch Portal*.
3. Complete the options to register FortiGate on FortiCare.

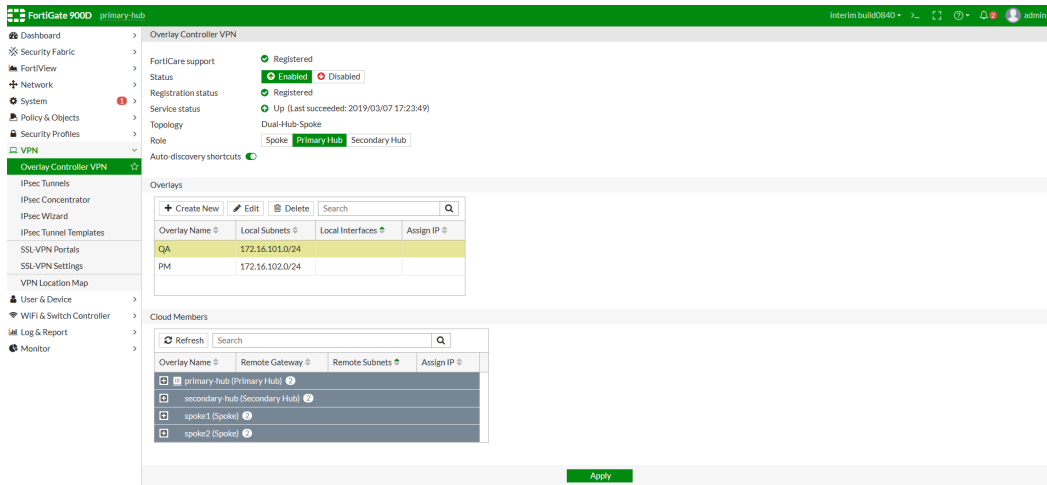
### To enable hub-spoke OCVPN using the GUI:

1. Go to *VPN > Overlay Controller VPN*.
2. Configure the OCVPN primary hub by setting the following options:
  - a. For *Status*, click *Enabled*.
  - b. For *Role*, click *Primary Hub*.
  - c. In the *Overlays* section, click *Create New* to create a network overlay.

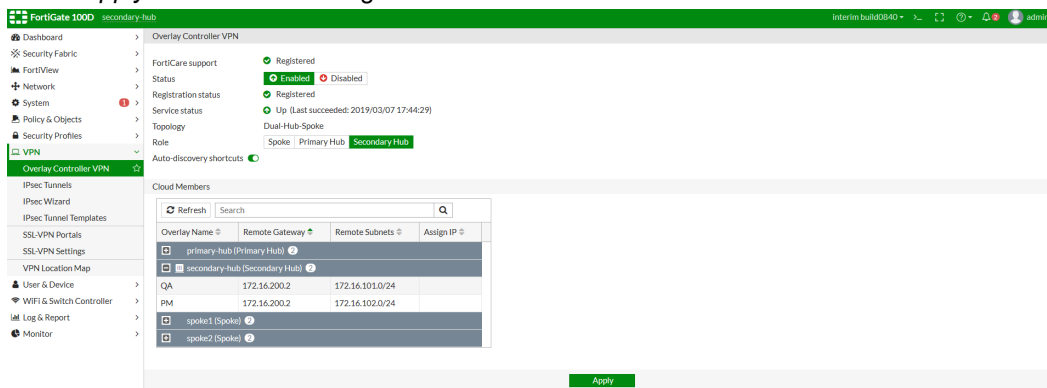


- d. Specify the *Name*, *Local subnets*, and/or *Local interfaces*. Then click *OK*.

- e. Click *Apply* to commit the configuration.



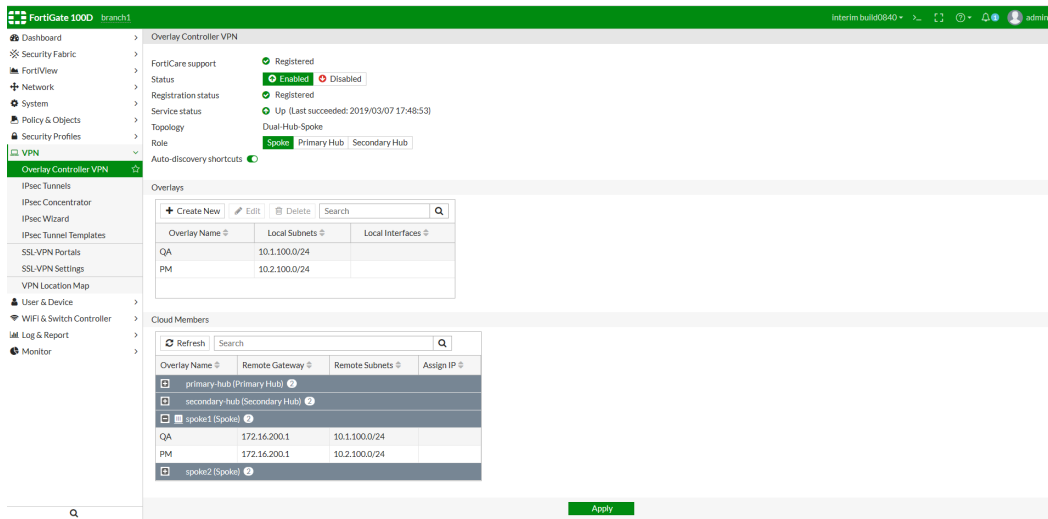
3. Configure the OCVPN secondary hub:
- Overlays are synced from the primary hub and cannot be defined in the secondary hub.
- In the *Overlay Controller VPN* pane, select *Secondary Hub* for the *Role*.
  - Select *Apply* to commit the configuration.



4. Configure the OCVPN spokes:
- In the *Overlay Controller VPN* pane, select *Spoke* for the *Role*.
  - In the *Overlays* section, click *Create New* to create a network overlay.
  - Specify the *Name*, *Local subnets*, and/or *Local interfaces*.  
The local subnet must be routable and interfaces must have IP addresses.



- d. Click **OK** and then click **Apply** to commit the configuration.



## To enable hub-spoke OCVPN using the CLI:

1. Configure the OCVPN primary hub:

```
config vpn ocvpn
 set status enable
 set role primary-hub
 config overlays
 edit 1
 set name "QA"
 config subnets
 edit 1
 set subnet 172.16.101.0 255.255.255.0
 next
 end
 next
 edit 2
 set name "PM"
 config subnets
 edit 1
 set subnet 172.16.102.0 255.255.255.0
 next
 end
 next
 end
end
```

2. Configure the OCVPN secondary hub:

```
config vpn ocvpn
 set status enable
 set role secondary-hub
end
```

3. Configure the OCVPN spoke1:

```
config vpn ocvpn
 set status enable
```

```
config overlays
 edit 1
 set name "QA"
 config subnets
 edit 1
 set subnet 10.1.100.0 255.255.255.0
 next
 end
 next
 edit 2
 set name "PM"
 config subnets
 edit 1
 set subnet 10.2.100.0 255.255.255.0
 next
 end
 next
end
end
```

#### 4. Configure the OCVPN spoke2:

```
config vpn ocvpn
 set status enable
 config overlays
 edit 1
 set name "QA"
 config subnets
 edit 1
 set subnet 192.168.4.0 255.255.255.0
 next
 end
 next
 edit 2
 set name "PM"
 config subnets
 edit 1
 set subnet 192.168.5.0 255.255.255.0
 next
 end
 next
 end
end
```

## Hub-spoke OCVPN with inter-overlay source NAT

This topic shows a sample configuration of hub-spoke OCVPN with inter-overlay source NAT. OCVPN isolates traffic between overlays by default. With NAT enabled on spokes and `assign-ip` enabled on hub, you can have inter-overlay communication.

Inter-overlay communication means devices from any source addresses and any source interfaces can communicate with any devices in overlays' subnets when the overlay option `assign-ip` is enabled.

You must first disable `auto-discovery` before you can enable NAT.

## License

- Free license: Hub-spoke network topology not supported.
- Full License: Maximum of 2 hubs, 10 overlays, 64 subnets per overlay; 512 spokes, 10 overlays, 16 subnets per overlay.

## Prerequisites

- All FortiGates must be running FortiOS 6.2.0 or later.
- All FortiGates must have Internet access.
- All FortiGates must be registered on FortiCare using the same FortiCare account.

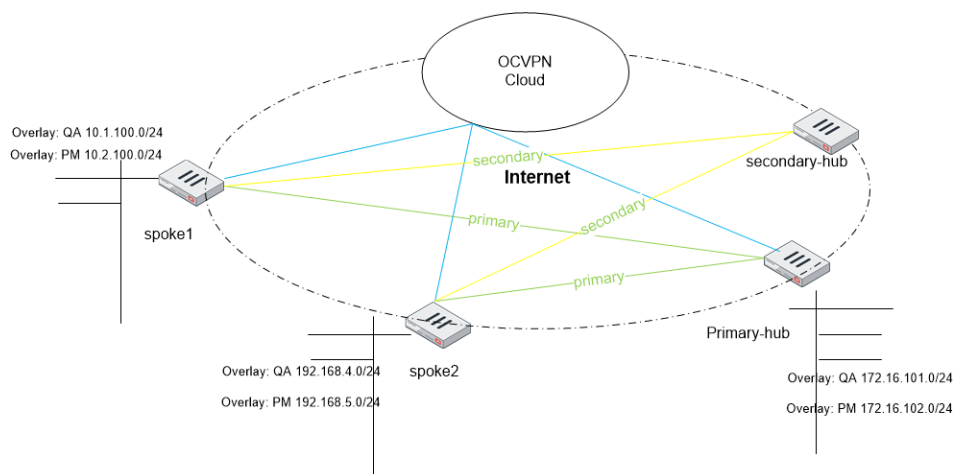
## Restrictions

- Non-root VDOMs do not support OCVPN.
- FortiOS 6.2.x is not compatible with FortiOS 6.0.x.

## OCVPN device roles

- Primary hub.
- Secondary hub.
- Spoke (OCVPN default role).

## Sample topology



## Sample configuration

You can only configure this feature using the CLI.



The overlay names on each device must be the same for local and remote selector pairs to be negotiated.

**To enable inter-overlay source NAT using the CLI:****1. Configure the primary hub, enable overlay QA, and configure assign-ip and IP range:**

```
config vpn ocvpn
 set status enable
 set role primary-hub
 config overlays
 edit 1
 set name "QA"
 set assign-ip enable
 set ipv4-start-ip 172.16.101.100
 set ipv4-end-ip 172.16.101.200
 config subnets
 edit 1
 set subnet 172.16.101.0 255.255.255.0
 next
 end
 next
 edit 2
 set name "PM"
 set assign-ip enable
 config subnets
 edit 1
 set subnet 172.16.102.0 255.255.255.0
 next
 end
 next
end
end
```

**2. Configure the secondary hub:**

```
config vpn ocvpn
 set status enable
 set role secondary-hub
end
```

**3. Configure spoke1 and enable NAT on the spoke:**

```
config vpn ocvpn
 set status enable
 set auto-discovery disable
 set nat enable
 config overlays
 edit 1
 set name "QA"
 config subnets
 edit 1
 set subnet 10.1.100.0 255.255.255.0
 next
 end
 next
 edit 2
 set name "PM"
 config subnets
 edit 1
 set subnet 10.2.100.0 255.255.255.0
```

```
 next
 end
 next
 end
end
```

#### 4. Configure spoke2 and enable NAT on the spoke:

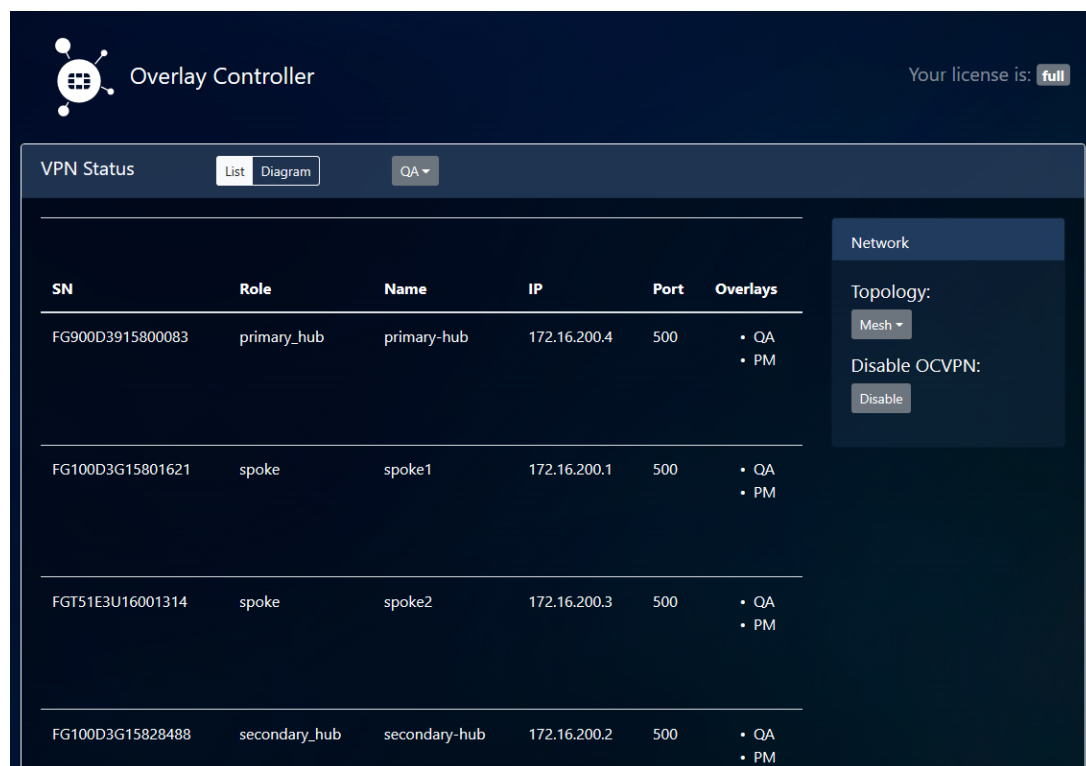
```
config vpn ocvpn
 set status enable
 set auto-discovery disable
 set nat enable
 config overlays
 edit 1
 set name "QA"
 config subnets
 edit 1
 set subnet 192.168.4.0 255.255.255.0
 next
 end
 next
 edit 2
 set name "PM"
 config subnets
 edit 1
 set subnet 192.168.5.0 255.255.255.0
 next
 end
 next
 end
end
```

#### A firewall policy with NAT is generated on the spoke:

```
edit 9
 set name "_OCVPN2-1.1_nat"
 set uuid 3f7a84b8-3d36-51e9-ee97-8f418c91e666
 set srcintf "any"
 set dstintf "_OCVPN2-1.1"
 set srcaddr "all"
 set dstaddr "_OCVPN2-1.1_remote_networks"
 set action accept
 set schedule "always"
 set service "ALL"
 set comments "Generated by OCVPN Cloud Service."
 set nat enable
next
```

## OCVPN portal

When you log into the OCVPN portal, the OCVPN license type and device information display. The device information includes the device serial number, OCVPN role, hostname, public IP address, port number, and overlays.



Overlay Controller

Your license is: **full**

VPN Status List Diagram QA

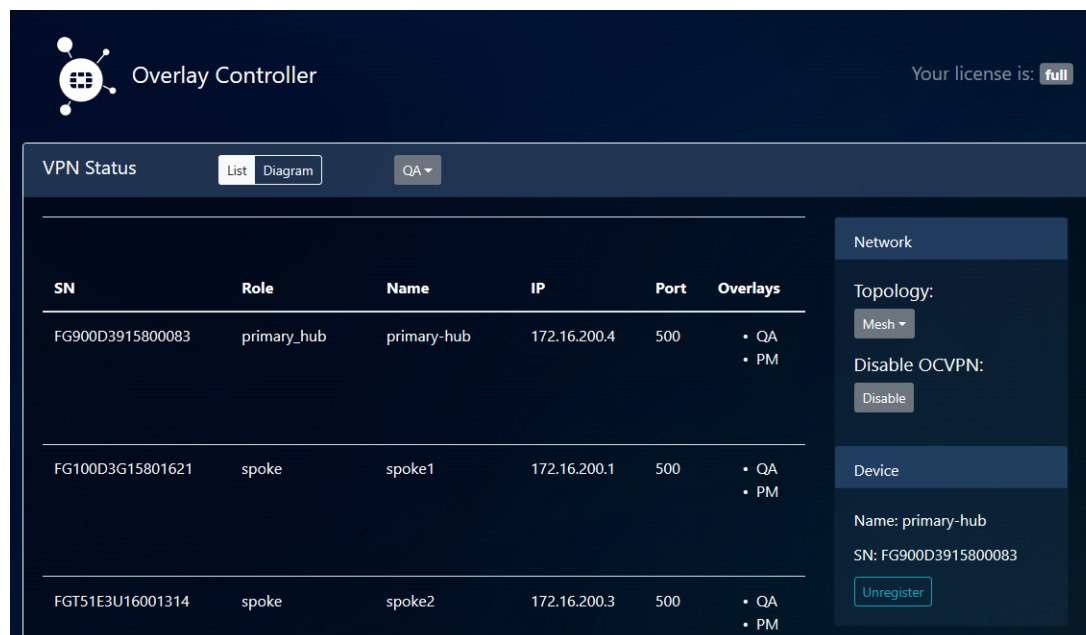
SN	Role	Name	IP	Port	Overlays
FG900D3915800083	primary_hub	primary-hub	172.16.200.4	500	• QA • PM
FG100D3G15801621	spoke	spoke1	172.16.200.1	500	• QA • PM
FGT51E3U16001314	spoke	spoke2	172.16.200.3	500	• QA • PM
FG100D3G15828488	secondary_hub	secondary-hub	172.16.200.2	500	• QA • PM

Network

Topology:  
Mesh

Disable OCVPN:  
Disable

You can unregister an OCVPN device from the OCVPN portal under *Device* on the right pane.



Overlay Controller

Your license is: **full**

VPN Status List Diagram QA

SN	Role	Name	IP	Port	Overlays
FG900D3915800083	primary_hub	primary-hub	172.16.200.4	500	• QA • PM
FG100D3G15801621	spoke	spoke1	172.16.200.1	500	• QA • PM
FGT51E3U16001314	spoke	spoke2	172.16.200.3	500	• QA • PM

Network

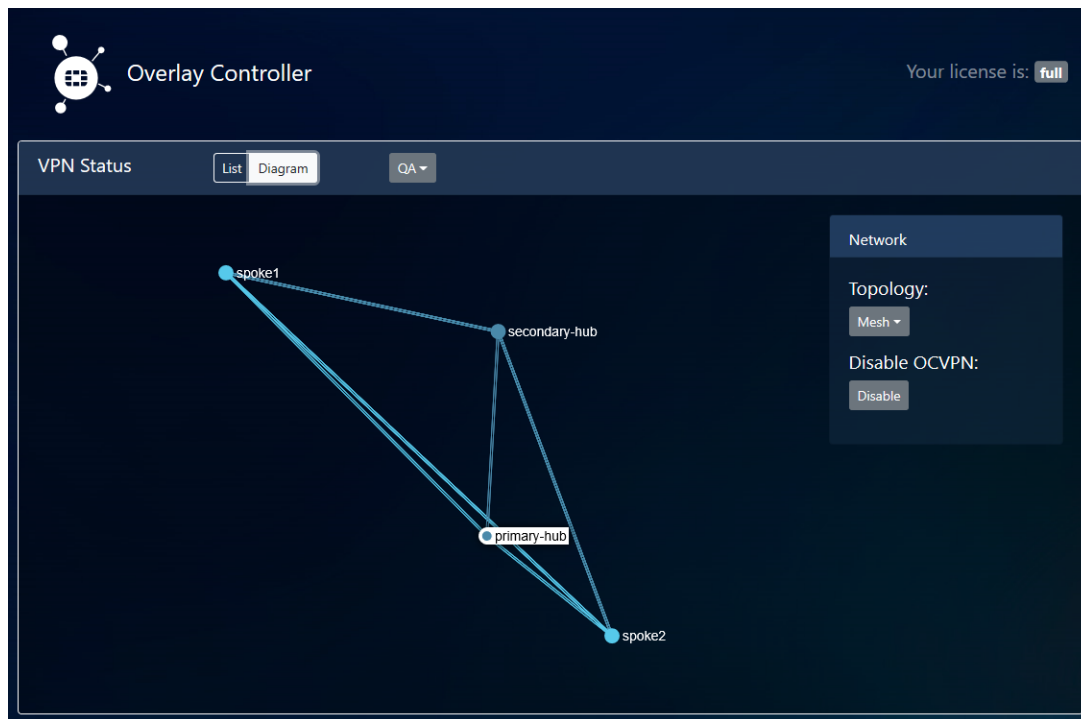
Topology:  
Mesh

Disable OCVPN:  
Disable

Device

Name: primary-hub  
SN: FG900D3915800083  
Unregister

Use the OCVPN *Diagram* to show the OCVPN network topology.



## Troubleshooting OCVPN

This document includes troubleshooting steps for the following OCVPN network topologies:

- Full mesh OCVPN.
- Hub-spoke OCVPN with ADVPN shortcut.
- Hub-spoke OCVPN with inter-overlay source NAT.

For OCVPN configurations in other network topologies, see the other OCVPN topics.

### Troubleshooting full mesh network topology

- `Branch_1#diagnose vpn ocvpn status`

```
Current State : Registered
Topology : Full-Mesh
Role : Spoke
Server Status : Up
Registration time : Thu Feb 28 18:42:25 2019
Update time : Thu Feb 28 15:57:18 2019
Poll time : Fri Mar 1 15:02:28 2019
```

- `Branch_1#diagnose vpn ocvpn show-meta`

```
Topology :: auto
License :: full
Members :: 3
Max-free :: 3
```

- Branch\_1#diagnose vpn ocvpn show-overlays

QA

PM

- Branch\_1#diagnose vpn ocvpn show-members

```
Member: { "SN": "FG100D3G15801621", "IPv4": "172.16.200.1", "port": "500", "slot": 1000,
"overlay": [{ "id": 0, "name": "QA", "subnets": ["10.1.100.0\255.255.255.0"], "ip_
range": "0.0.0.0-0.0.0.0" }, { "id": 1, "name": "PM", "subnets": [
"10.2.100.0\255.255.255.0"], "ip_range": "0.0.0.0-0.0.0.0" }], "Name": "FortiGate-
100D", "topology_role": "spoke" }
Member: { "SN": "FG900D3915800083", "IPv4": "172.16.200.4", "port": "500", "slot": 1001,
"overlay": [{ "id": 0, "name": "QA", "subnets": ["172.16.101.0\255.255.255.0"], "ip_
range": "0.0.0.0-0.0.0.0" }, { "id": 1, "name": "PM", "subnets": [
"172.16.102.0\255.255.255.0"], "ip_range": "0.0.0.0-0.0.0.0" }], "Name": "Branch3",
"topology_role": "spoke" }
Member: { "SN": "FGT51E3U16001314", "IPv4": "172.16.200.199", "port": "500", "slot":
1002, "overlay": [{ "id": 0, "name": "QA", "subnets": ["192.168.4.0\255.255.255.0"],
"ip_range": "0.0.0.0-0.0.0.0" }, { "id": 1, "name": "PM", "subnets": [
"192.168.5.0\255.255.255.0"], "ip_range": "0.0.0.0-0.0.0.0" }], "Name": "Branch2",
"topology_role": "spoke" }
```

- Branch\_1#diagnose vpn tunnel list

list all ipsec tunnel in vd 0

```

name=_OCVPN2-3.1 ver=2 serial=4 172.16.200.1:0->172.16.200.199:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=1
```

```
proxyid_num=2 child_num=0 refcnt=13 ilast=7 olast=0 ad=/0
stat: rxp=0 txp=7 rxb=0 txb=588
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=6
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-3.1 proto=0 sa=1 ref=2 serial=8 auto-negotiate
src: 0:10.1.100.0-10.1.100.255:0
dst: 0:192.168.4.0-192.168.4.255:0
SA: ref=3 options=18627 type=00 soft=0 mtu=1438 expire=42923/0B replaywin=2048
seqno=8 esn=0 replaywin_lastseq=00000000 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42931/43200
dec: spi=c34bb752 esp=aes key=16 3c5ceeff3cac1eaa2702b5ccb713ab9b
ah=sha1 key=20 5903e358b3d8938ee64f0412887a0fe741ccb105
enc: spi=b5bd4fel esp=aes key=16 8ae97a8abe24dae725d614d2a6efdcdb0
ah=sha1 key=20 9ec200d9c0cef9e1b7cf76e05dbf344c70f53214
dec:pkts/bytes=0/0, enc:pkts/bytes=7/1064
proxyid=_OCVPN2-3.1 proto=0 sa=0 ref=2 serial=1 auto-negotiate
src: 0:10.1.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0
```

```

name=_OCVPN2-4.1 ver=2 serial=6 172.16.200.1:0->172.16.200.4:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=1
```

```
proxyid_num=2 child_num=0 refcnt=11 ilast=19 olast=19 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
```



```
proxyid=_OCVPN2-4.1 proto=0 sa=1 ref=2 serial=7 auto-negotiate
src: 0:10.1.100.0-10.1.100.255:0
dst: 0:172.16.101.0-172.16.101.255:0
SA: ref=3 options=18627 type=00 soft=0 mtu=1438 expire=42911/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42931/43200
dec: spi=c34bb750 esp=aes key=16 8c9844a8bcd3fda6c7bd8a4f2ec81ef1
ah=sha1 key=20 680c7144346f5b52126cbad9f325821b048c7192
enc: spi=f2d1f2d4 esp=aes key=16 f9625fc8590152829eb39eecab3a3999
ah=sha1 key=20 5df8447416da541fa54dde9fa3e5c35fbfc4723f
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
proxyid=_OCVPN2-4.1 proto=0 sa=0 ref=2 serial=1 auto-negotiate
src: 0:10.1.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0

name=_OCVPN2-3.2 ver=2 serial=3 172.16.200.1:0->172.16.200.199:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=1

proxyid_num=2 child_num=0 refcnt=11 ilast=6 olast=6 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-3.2 proto=0 sa=1 ref=2 serial=8 auto-negotiate
src: 0:10.2.100.0-10.2.100.255:0
dst: 0:192.168.5.0-192.168.5.255:0
SA: ref=3 options=18627 type=00 soft=0 mtu=1438 expire=42923/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42930/43200
dec: spi=c34bb753 esp=aes key=16 58ddfad9a3699f1c49f3a9f369145c28
ah=sha1 key=20 e749c7e6a7aaff119707c792eb73cd975127873b
enc: spi=b5bd4fe2 esp=aes key=16 8f2366e653f5f9ad6587belce1905764
ah=sha1 key=20 5347bf24e51219d483c0f7b058eceab202026204
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
proxyid=_OCVPN2-3.2 proto=0 sa=0 ref=2 serial=1 auto-negotiate
src: 0:10.2.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0

name=_OCVPN2-4.2 ver=2 serial=5 172.16.200.1:0->172.16.200.4:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=1

proxyid_num=2 child_num=0 refcnt=11 ilast=17 olast=17 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-4.2 proto=0 sa=1 ref=2 serial=7 auto-negotiate
src: 0:10.2.100.0-10.2.100.255:0
dst: 0:172.16.102.0-172.16.102.255:0
SA: ref=3 options=18627 type=00 soft=0 mtu=1438 expire=42905/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42927/43200
dec: spi=c34bb751 esp=aes key=16 41449ee5ea43d3e1f80df05fc632cd44
ah=sha1 key=20 3ca2aealc8764f35ccf987cdeca7cf6eb54331fb
enc: spi=f2d1f2d5 esp=aes key=16 9010dd57e502c6296b27a4649a45a6ba
ah=sha1 key=20 caf86a176ce04464221543f15fc3c63fc573b8ee
```

```

dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
proxyid=_OCVPN2-4.2 proto=0 sa=0 ref=2 serial=1 auto-negotiate
src: 0:10.2.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0

```

- **Branch\_1#**get router info routing-table all

```

Routing table for VRF=0
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
 O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default

S* 0.0.0.0/0 [10/0] via 172.16.200.254, port1
C 10.1.100.0/24 is directly connected, dmz
C 10.2.100.0/24 is directly connected, loop
C 11.101.1.0/24 is directly connected, wan1
C 11.102.1.0/24 is directly connected, wan2
S 192.168.5.0/24 [20/0] is directly connected, _OCVPN2-3.2
C 172.16.200.0/24 is directly connected, port1
S 172.16.101.0/24 [20/0] is directly connected, _OCVPN2-4.1
S 172.16.102.0/24 [20/0] is directly connected, _OCVPN2-4.2
S 192.168.4.0/24 [20/0] is directly connected, _OCVPN2-3.1

```

## Troubleshooting hub-spoke with ADVPN shortcut

- **Primary-Hub#**diagnose vpn ocvpn status

```

Current State : Registered
Topology : Dual-Hub-Spoke
Role : Primary-Hub
Server Status : Up
Registration time : Sat Mar 2 11:31:54 2019
Poll time : Sat Mar 2 11:46:02 2019

```

- **Spoke1#**diagnose vpn ocvpn status

```

Current State : Registered
Topology : Dual-Hub-Spoke
Role : Spoke
Server Status : Up
Registration time : Sat Mar 2 11:41:22 2019
Poll time : Sat Mar 2 11:46:44 2019

```

- **Primary-Hub#**diagnose vpn ocvpn show-members

```

Member: { "sn": "FG900D3915800083", "ip_v4": "172.16.200.4", "port": 500, "slot": 0,
"overlay": [{ "id": 0, "name": "QA", "subnets": ["172.16.101.0\255.255.255.0"], "ip_
range": "0.0.0.0-0.0.0.0" }, { "id": 1, "name": "PM", "subnets": [
"172.16.102.0\255.255.255.0"], "ip_range": "0.0.0.0-0.0.0.0" }], "name": "Primary-
Hub", "topology_role": "primary_hub", "eap": "disable", "auto_discovery": "enable" }
Member: { "sn": "FG100D3G15828488", "ip_v4": "172.16.200.2", "port": 500, "slot": 1,
"overlay": [{ "id": 0, "name": "QA", "subnets": ["172.16.101.0\255.255.255.0"], "ip_
range": "0.0.0.0-0.0.0.0" }, { "id": 1, "name": "PM", "subnets": [
"172.16.102.0\255.255.255.0"], "ip_range": "0.0.0.0-0.0.0.0" }], "name": "Secondary-
Hub", "topology_role": "secondary_hub", "eap": "disable", "auto_discovery": "enable" }

```

```
Member: { "sn": "FG100D3G15801621", "ip_v4": "172.16.200.1", "port": 500, "slot": 1000,
"overlay": [{ "id": 0, "name": "QA", "subnets": ["10.1.100.0\255.255.255.0"], "ip_
range": "0.0.0.0-0.0.0.0" }, { "id": 1, "name": "PM", "subnets": [
"10.2.100.0\255.255.255.0"], "ip_range": "0.0.0.0-0.0.0.0" }], "name": "Spoke1",
"topology_role": "spoke" }
Member: { "sn": "FGT51E3U16001314", "ip_v4": "172.16.200.3", "port": 500, "slot": 1001,
"overlay": [{ "id": 0, "name": "QA", "subnets": ["192.168.4.0\255.255.255.0"], "ip_
range": "0.0.0.0-0.0.0.0" }, { "id": 1, "name": "PM", "subnets": [
"192.168.5.0\255.255.255.0"], "ip_range": "0.0.0.0-0.0.0.0" }], "name": "Spoke2",
"topology_role": "spoke" }
```

- **Primary-Hub#**diagnose vpn ocvpn show-meta

```
Topology :: auto
License :: full
Members :: 4
Max-free :: 3
```

- **Primary-Hub#**diagnose vpn ocvpn show-overlays

```
QA
PM
```

- **Spoke1#**diagnose vpn tunnel list

```
list all ipsec tunnel in vd 0
```

```

name=_OCVPN2-0.0 ver=2 serial=6 172.16.200.1:0->172.16.200.4:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=1
```

```
proxyid_num=1 child_num=0 refcnt=11 ilast=0 olast=0 ad=r/2
stat: rxp=1 txp=34 rxb=152 txb=2856
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=46
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-0.0 proto=0 sa=1 ref=2 serial=1 auto-negotiate adr
src: 0:10.1.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=3 options=1a227 type=00 soft=0 mtu=1438 expire=42895/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42901/43200
dec: spi=048477c7 esp=aes key=16 240e064c0f1c980ca31980b9e7605c9d
ah=sha1 key=20 6ff022cbebc4ff4c5de62eefb2e6180c40a3adb2
enc: spi=dfcffa86 esp=aes key=16 862208de164a02af377756c2bcabd588
ah=sha1 key=20 af6e54781fd42d7a2ba2119ec95d0f95629c8448
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

```

name=_OCVPN2-1.0 ver=2 serial=8 172.16.200.1:0->172.16.200.2:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=0
```

```
proxyid_num=1 child_num=0 refcnt=10 ilast=934 olast=934 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=20000ms retry=3 count=0 seqno=1
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-1.0 proto=0 sa=0 ref=2 serial=1 auto-negotiate adr
src: 0:10.1.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0
```

```

name=_OCVPN2-0.1 ver=2 serial=5 172.16.200.1:0->172.16.200.4:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=1

```

```

proxyid_num=1 child_num=0 refcnt=11 ilast=12 olast=12 ad=r/2
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=46
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-0.1 proto=0 sa=1 ref=2 serial=1 auto-negotiate adr
src: 0:10.2.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=3 options=1a227 type=00 soft=0 mtu=1438 expire=42895/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42901/43200
dec: spi=048477c8 esp=aes key=16 701ec608767f4988b76c2f662464e654
ah=sha1 key=20 93c65d106dc610d7ee3f04487f08601a9e00ffdd
enc: spi=dfcffa87 esp=aes key=16 02b2d04dce3d81ebab69e128d45cb7ca
ah=sha1 key=20 4a9283847f852c83a75691fad44d07d8409a2267
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0

```

```

name=_OCVPN2-1.1 ver=2 serial=7 172.16.200.1:0->172.16.200.2:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=0

```

```

proxyid_num=1 child_num=0 refcnt=10 ilast=934 olast=934 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=20000ms retry=3 count=0 seqno=1
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-1.1 proto=0 sa=0 ref=2 serial=1 auto-negotiate adr
src: 0:10.2.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0

```

- **Spoke1 #get router info routing-table all**

```

Routing table for VRF=0
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default

```

```

S* 0.0.0.0/0 [10/0] via 172.16.200.254, port1
C 10.1.100.0/24 is directly connected, dmz
C 10.2.100.0/24 is directly connected, loop
C 11.101.1.0/24 is directly connected, wan1
C 11.102.1.0/24 is directly connected, wan2
S 172.16.102.0/24 [20/0] is directly connected, _OCVPN2-0.1
C 172.16.200.0/24 is directly connected, port1
S 172.16.101.0/24 [20/0] is directly connected, _OCVPN2-0.0
S 192.168.4.0/24 [20/0] is directly connected, _OCVPN2-0.0
S 192.168.5.0/24 [20/0] is directly connected, _OCVPN2-0.1

```

- **Generate traffic from spoke1 to spoke2 to trigger the ADVPN shortcut and check the VPN tunnel and routing-table again on spoke1.**

```

branch1 # diagnose vpn tunnel list
list all ipsec tunnel in vd 0

name=_OCVPN2-0.0_0 ver=2 serial=a 172.16.200.1:0->172.16.200.3:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/720 options
[02d0]=create_dev no-sysctl rgwy-chg frag-rfc accept_traffic=1

parent=_OCVPN2-0.0 index=0
proxyid_num=1 child_num=0 refcnt=14 ilast=0 olast=0 ad=r/2
stat: rxp=7 txp=7 rxb=1064 txb=588
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-0.0 proto=0 sa=1 ref=2 serial=1 auto-negotiate add-route adr
src: 0:10.1.100.0-10.1.100.255:0
dst: 0:192.168.4.0-192.168.4.255:0
SA: ref=3 options=1a227 type=00 soft=0 mtu=1438 expire=43180/0B replaywin=2048
seqno=8 esn=0 replaywin_lastseq=00000008 itn=0 qat=0
life: type=01 bytes=0/0 timeout=43187/43200
dec: spi=048477c9 esp=aes key=16 27c35d53793013ef24cf887561e9f313
ah=sha1 key=20 2c8cfd328c3b29104db0ca74a00c6063f46cafe4
enc: spi=fb9e13fd esp=aes key=16 9d0d3bf6c84b7ddaf9d9196fe74002ed
ah=sha1 key=20 d1f541db787dea384c6a4df16fc228abeb7ae334
dec:pkts/bytes=7/588, enc:pkts/bytes=7/1064

name=_OCVPN2-0.0 ver=2 serial=6 172.16.200.1:0->172.16.200.4:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=1

proxyid_num=1 child_num=1 refcnt=12 ilast=7 olast=7 ad=r/2
stat: rxp=2 txp=35 rxb=304 txb=2940
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=65
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-0.0 proto=0 sa=1 ref=2 serial=1 auto-negotiate adr
src: 0:10.1.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=3 options=1a227 type=00 soft=0 mtu=1438 expire=42500/0B replaywin=2048
seqno=2 esn=0 replaywin_lastseq=00000002 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42901/43200
dec: spi=048477c7 esp=aes key=16 240e064c0f1c980ca31980b9e7605c9d
ah=sha1 key=20 6ff022cbebc4ff4c5de62eefb2e6180c40a3adb2
enc: spi=dfcffa86 esp=aes key=16 862208de164a02af377756c2bcabd588
ah=sha1 key=20 af6e54781fd42d7a2ba2119ec95d0f95629c8448
dec:pkts/bytes=1/84, enc:pkts/bytes=1/152

name=_OCVPN2-1.0 ver=2 serial=8 172.16.200.1:0->172.16.200.2:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=0

proxyid_num=1 child_num=0 refcnt=10 ilast=1328 olast=1328 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=20000ms retry=3 count=0 seqno=1
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-1.0 proto=0 sa=0 ref=2 serial=1 auto-negotiate adr
src: 0:10.1.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0

```

```
name=_OCVPN2-0.1 ver=2 serial=5 172.16.200.1:0->172.16.200.4:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=1
```

```
proxyid_num=1 child_num=0 refcnt=11 ilast=5 olast=5 ad=r/2
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=66
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-0.1 proto=0 sa=1 ref=2 serial=1 auto-negotiate adr
src: 0:10.2.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=3 options=1a227 type=00 soft=0 mtu=1438 expire=42500/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42901/43200
dec: spi=048477c8 esp=aes key=16 701ec608767f4988b76c2f662464e654
ah=sha1 key=20 93c65d106dc610d7ee3f04487f08601a9e00ffdd
enc: spi=dfcffa87 esp=aes key=16 02b2d04dce3d81ebab69e128d45cb7ca
ah=sha1 key=20 4a9283847f852c83a75691fad44d07d8409a2267
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

```

name=_OCVPN2-1.1 ver=2 serial=7 172.16.200.1:0->172.16.200.2:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=0
```

```
proxyid_num=1 child_num=0 refcnt=10 ilast=1328 olast=1328 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=20000ms retry=3 count=0 seqno=1
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-1.1 proto=0 sa=0 ref=2 serial=1 auto-negotiate adr
src: 0:10.2.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0
```

Routing table for VRF=0

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP  
O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2  
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
\* - candidate default

```
S* 0.0.0.0/0 [10/0] via 172.16.200.254, port1
C 10.1.100.0/24 is directly connected, dmz
C 10.2.100.0/24 is directly connected, loop
C 11.101.1.0/24 is directly connected, wan1
C 11.102.1.0/24 is directly connected, wan2
S 172.16.102.0/24 [20/0] is directly connected, _OCVPN2-0.1
C 172.16.200.0/24 is directly connected, port1
S 172.16.101.0/24 [20/0] is directly connected, _OCVPN2-0.0
S 192.168.4.0/24 [15/0] via 172.16.200.3, _OCVPN2-0.0_0
S 192.168.5.0/24 [20/0] is directly connected, _OCVPN2-0.1
```

- Simulate the primary hub being unavailable where all spokes' dialup VPN tunnels will switch to the secondary hub, to check VPN tunnel status and routing-table.

```
list all ipsec tunnel in vd 0
```

```

```

```
name=_OCVPN2-0.0 ver=2 serial=6 172.16.200.1:0->172.16.200.4:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=0

proxyid_num=1 child_num=0 refcnt=10 ilast=25 olast=25 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=20000ms retry=3 count=0 seqno=82
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-0.0 proto=0 sa=0 ref=2 serial=1 auto-negotiate adr
src: 0:10.1.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0

name=_OCVPN2-1.0 ver=2 serial=8 172.16.200.1:0->172.16.200.2:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=1

proxyid_num=1 child_num=0 refcnt=11 ilast=14 olast=14 ad=r/2
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=9
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-1.0 proto=0 sa=1 ref=2 serial=1 auto-negotiate adr
src: 0:10.1.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=3 options=1a227 type=00 soft=0 mtu=1438 expire=42723/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42898/43200
dec: spi=048477cd esp=aes key=16 9bb363a32378b5897cd42890c92df811
ah=sha1 key=20 2ed40583b9544e37867349b4adc7c013024d7e17
enc: spi=f345fb42 esp=aes key=16 3ea31dff3310b245700a131db4565851
ah=sha1 key=20 522862dfb232514b845e436133b148da0e67b7c4
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0

name=_OCVPN2-0.1 ver=2 serial=5 172.16.200.1:0->172.16.200.4:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=0

proxyid_num=1 child_num=0 refcnt=10 ilast=19 olast=19 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=20000ms retry=3 count=0 seqno=83
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-0.1 proto=0 sa=0 ref=2 serial=1 auto-negotiate adr
src: 0:10.2.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0

name=_OCVPN2-1.1 ver=2 serial=7 172.16.200.1:0->172.16.200.2:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=1

proxyid_num=1 child_num=0 refcnt=11 ilast=12 olast=12 ad=r/2
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=9
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-1.1 proto=0 sa=1 ref=2 serial=1 auto-negotiate adr
src: 0:10.2.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=3 options=1a227 type=00 soft=0 mtu=1438 expire=42728/0B replaywin=2048
```

```

seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42902/43200
dec: spi=048477cf esp=aes key=16 b6f0ca7564abcd8559b5b0ebb3fd04c1
 ah=sha1 key=20 4130d040554b39daca72adac7583b9cc83cce3c8
enc: spi=f345fb43 esp=aes key=16 727582f20fcedff884ba693ed2164bcd
 ah=sha1 key=20 b0a625803fde701ed9d28d256079e908954b7fc8
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0

```

Routing table for VRF=0

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP  
 O - OSPF, IA - OSPF inter area  
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
 E1 - OSPF external type 1, E2 - OSPF external type 2  
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area  
 \* - candidate default

```

S* 0.0.0.0/0 [10/0] via 172.16.200.254, port1
C 10.1.100.0/24 is directly connected, dmz
C 10.2.100.0/24 is directly connected, loop
C 11.101.1.0/24 is directly connected, wan1
C 11.102.1.0/24 is directly connected, wan2
S 172.16.102.0/24 [21/0] is directly connected, _OCVPN2-1.1
C 172.16.200.0/24 is directly connected, port1
S 172.16.101.0/24 [21/0] is directly connected, _OCVPN2-1.0
S 192.168.4.0/24 [21/0] is directly connected, _OCVPN2-1.0
S 192.168.5.0/24 [21/0] is directly connected, _OCVPN2-1.1

```

## Troubleshooting hub-spoke with inter-overlay source NAT

- Primary-Hub #diagnose vpn ocvpn status

```

Current State : Registered
Topology : Dual-Hub-Spoke
Role : Primary-Hub
Server Status : Up
Registration time : Sat Mar 2 11:31:54 2019
Update time : Sat Mar 2 13:57:05 2019
Poll time : Sat Mar 2 14:03:31 2019

```

- Spoke1 #diagnose vpn ocvpn status

```

Current State : Registered
Topology : Dual-Hub-Spoke
Role : Spoke
Server Status : Up
Registration time : Sat Mar 2 13:58:01 2019
Poll time : Sat Mar 2 14:04:22 2019

```

- Primary-Hub #diagnose vpn ocvpn show-members

```

Member: { "sn": "FG900D3915800083", "ip_v4": "172.16.200.4", "port": 500, "slot": 0,
"overlay": [{ "id": 0, "name": "QA", "subnets": ["172.16.101.0\255.255.255.0"], "ip_
range": "172.16.101.100-172.16.101.200" }, { "id": 1, "name": "PM", "subnets": [
"172.16.102.0\255.255.255.0"], "ip_range": "172.16.102.100-172.16.102.200" }],
"name": "Primary-Hub", "topology_role": "primary_hub", "eap": "disable", "auto_
discovery": "enable" }
Member: { "sn": "FG100D3G15828488", "ip_v4": "172.16.200.2", "port": 500, "slot": 1,

```



```
"overlay": [{ "id": 0, "name": "QA", "subnets": ["172.16.101.0\255.255.255.0"], "ip_range": "0.0.0.0-0.0.0.0" }, { "id": 1, "name": "PM", "subnets": ["172.16.102.0\255.255.255.0"], "ip_range": "0.0.0.0-0.0.0.0" }], "name": "Secondary-Hub", "topology_role": "secondary_hub", "eap": "disable", "auto_discovery": "enable" }
Member: { "sn": "FGT51E3U16001314", "ip_v4": "172.16.200.3", "port": 500, "slot": 1001, "overlay": [{ "id": 0, "name": "QA", "subnets": ["192.168.4.0\255.255.255.0"], "ip_range": "0.0.0.0-0.0.0.0" }, { "id": 1, "name": "PM", "subnets": ["192.168.5.0\255.255.255.0"], "ip_range": "0.0.0.0-0.0.0.0" }], "name": "Spoke2", "topology_role": "spoke" }
Member: { "sn": "FG100D3G15801621", "ip_v4": "172.16.200.1", "port": 500, "slot": 1000, "overlay": [{ "id": 0, "name": "QA", "subnets": ["10.1.100.0\255.255.255.0"], "ip_range": "0.0.0.0-0.0.0.0" }, { "id": 1, "name": "PM", "subnets": ["10.2.100.0\255.255.255.0"], "ip_range": "0.0.0.0-0.0.0.0" }], "name": "Spoke1", "topology_role": "spoke" }
```

- **Primary-Hub#**diagnose vpn ocvpn show-meta

```
Topology :: auto
License :: full
Members :: 4
Max-free :: 3
```

- **Primary-Hub#**diagnose vpn ocvpn show-overlays

```
QA
PM
```

- **Spoke1#**diagnose vpn tunnel list

```
list all ipsec tunnel in vd 0

name=_OCVPN2-0.0 ver=2 serial=c 172.16.200.1:0->172.16.200.4:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=1

proxyid_num=3 child_num=0 refcnt=13 ilast=17 olast=17 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=29
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-0.0 proto=0 sa=1 ref=2 serial=1 auto-negotiate
src: 0:10.1.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=3 options=18227 type=00 soft=0 mtu=1438 expire=42299/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42899/43200
dec: spi=0484795d esp=aes key=16 10eeb76fadd49f00c333350d83509095
ah=sha1 key=20 971bde5dcfca7e52fd1573cb3489e9c855f6154e
enc: spi=dfcffffaa esp=aes key=16 d07a4dd683ee093af2dca9485aa436eb
ah=sha1 key=20 65369be35d5ecad8cae63557318419cd6005c230
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
proxyid=_OCVPN2-0.0_nat proto=0 sa=1 ref=2 serial=3 auto-negotiate
src: 0:172.16.101.101-172.16.101.101:0
dst: 0:0.0.0.0-255.255.255.255:0
SA: ref=3 options=18627 type=00 soft=0 mtu=1438 expire=42303/0B replaywin=2048
seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42898/43200
dec: spi=04847961 esp=aes key=16 ea181036b02e8bc8711fb520b3e98a60
ah=sha1 key=20 b3c449d96d5d3f090975087a62447f6918ce7930
```

```

enc: spi=dfcffaac esp=aes key=16 f7ea5e42e9443698e6b8b32161ace40e
 ah=sha1 key=20 a7e36dd1ec0bdb6eff0aa66e442707427400c700
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
proxyid=_OCVPN2-0.0_nat proto=0 sa=0 ref=2 serial=2 auto-negotiate
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0

name=_OCVPN2-1.0 ver=2 serial=e 172.16.200.1:0->172.16.200.2:0 dst_mtu=0
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=1

proxyid_num=2 child_num=0 refcnt=10 ilast=599 olast=599 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-1.0 proto=0 sa=0 ref=2 serial=1 auto-negotiate
src: 0:10.1.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0
proxyid=_OCVPN2-1.0_nat proto=0 sa=0 ref=2 serial=2 auto-negotiate
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0

name=_OCVPN2-0.1 ver=2 serial=b 172.16.200.1:0->172.16.200.4:0 dst_mtu=1500
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=1

proxyid_num=3 child_num=0 refcnt=13 ilast=17 olast=17 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=1 idle=20000ms retry=3 count=0 seqno=29
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-0.1 proto=0 sa=1 ref=2 serial=1 auto-negotiate
src: 0:10.2.100.0/255.255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=3 options=18227 type=00 soft=0 mtu=1438 expire=42297/0B replaywin=2048
 seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42897/43200
dec: spi=0484795e esp=aes key=16 106eaa95a2be64b566e7d1ca0aa88f6a
 ah=sha1 key=20 5dddfba7070b03d5a31931d41db06ff96e7bc542
enc: spi=dfcffaab esp=aes key=16 29c774dbd7e54464ee298c381e71a94e
 ah=sha1 key=20 c3da7372789c0a53b3752e69baabala42d798820
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
proxyid=_OCVPN2-0.1_nat proto=0 sa=1 ref=2 serial=3 auto-negotiate
src: 0:172.16.102.101-172.16.102.101:0
dst: 0:0.0.0.0-255.255.255.255:0
SA: ref=3 options=18627 type=00 soft=0 mtu=1438 expire=42307/0B replaywin=2048
 seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0
life: type=01 bytes=0/0 timeout=42902/43200
dec: spi=04847962 esp=aes key=16 b7daa5807cfa86906592a012a9d2478f
 ah=sha1 key=20 39c8bb4c9e3f1e9e451f22c58a172ff01155055d
enc: spi=dfcffaad esp=aes key=16 2ecc644def4cebe6b0c4b7729da43d8e
 ah=sha1 key=20 469c6f319e83bd73468f55d430566afcd6215138
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
proxyid=_OCVPN2-0.1_nat proto=0 sa=0 ref=2 serial=2 auto-negotiate
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0

```

```
name=_OCVPN2-1.1 ver=2 serial=d 172.16.200.1:0->172.16.200.2:0 dst_mtu=0
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/528 options[0210]=create_dev
frag-rfc accept_traffic=1
```

```
proxyid_num=2 child_num=0 refcnt=10 ilast=599 olast=599 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=_OCVPN2-1.1 proto=0 sa=0 ref=2 serial=1 auto-negotiate
src: 0:10.2.100.0/255.255.0:0
dst: 0:0.0.0.0/0.0.0.0:0
proxyid=_OCVPN2-1.1_nat proto=0 sa=0 ref=2 serial=2 auto-negotiate
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
```

- Spoke1# get router info routing-table all

```
Routing table for VRF=0
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
 O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default
```

```
S* 0.0.0.0/0 [10/0] via 172.16.200.254, port1
C 10.1.100.0/24 is directly connected, dmz
C 10.2.100.0/24 is directly connected, loop
C 11.101.1.0/24 is directly connected, wan1
C 11.102.1.0/24 is directly connected, wan2
S 172.16.101.0/24 [20/0] is directly connected, _OCVPN2-0.1
C 172.16.101.101/32 is directly connected, _OCVPN2-0.1
C 172.16.200.0/24 is directly connected, port1
S 172.16.102.0/24 [20/0] is directly connected, _OCVPN2-0.0
C 172.16.102.101/32 is directly connected, _OCVPN2-0.0
S 192.168.4.0/24 [20/0] is directly connected, _OCVPN2-0.0
S 192.168.5.0/24 [20/0] is directly connected, _OCVPN2-0.1
```

- Spoke1# show firewall policy

```
.....
```

```
edit 9
 set name "_OCVPN2-1.1_nat"
 set uuid 3f7a84b8-3d36-51e9-ee97-8f418c91e666
 set srcintf "any"
 set dstintf "_OCVPN2-1.1"
 set srcaddr "all"
 set dstaddr "_OCVPN2-1.1_remote_networks"
 set action accept
 set schedule "always"
 set service "ALL"
 set comments "Generated by OCVPN Cloud Service."
 set nat enable
next
edit 12
 set name "_OCVPN2-1.0_nat"
```

```

set uuid 3fafec98-3d36-51e9-80c0-5d99325bad83
set srcintf "any"
set dstintf "_OCVPN2-1.0"
set srcaddr "all"
set dstaddr "_OCVPN2-1.0_remote_networks"
set action accept
set schedule "always"
set service "ALL"
set comments "Generated by OCVPN Cloud Service."
set nat enable
next
.....

```

## ADVPN

Auto-Discovery VPN (ADVPN) allows the central hub to dynamically inform spokes about a better path for traffic between two spokes.

The following topics provide instructions on configuring ADVPN:

- [IPsec VPN wizard hub-and-spoke ADVPN support on page 1310](#)
- [ADVPN with BGP as the routing protocol on page 1314](#)
- [ADVPN with OSPF as the routing protocol on page 1323](#)
- [ADVPN with RIP as the routing protocol on page 1332](#)

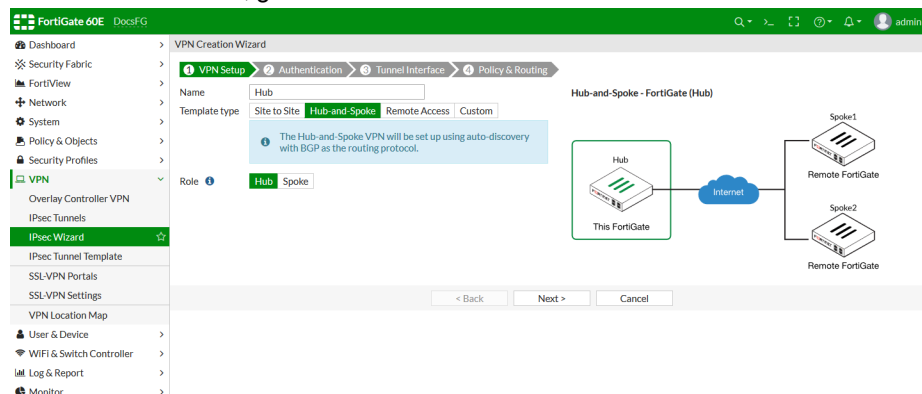
## IPsec VPN wizard hub-and-spoke ADVPN support

The IPsec Wizard can be used to create hub-and-spoke VPNs, with ADVPN enabled to establish tunnels between spokes.

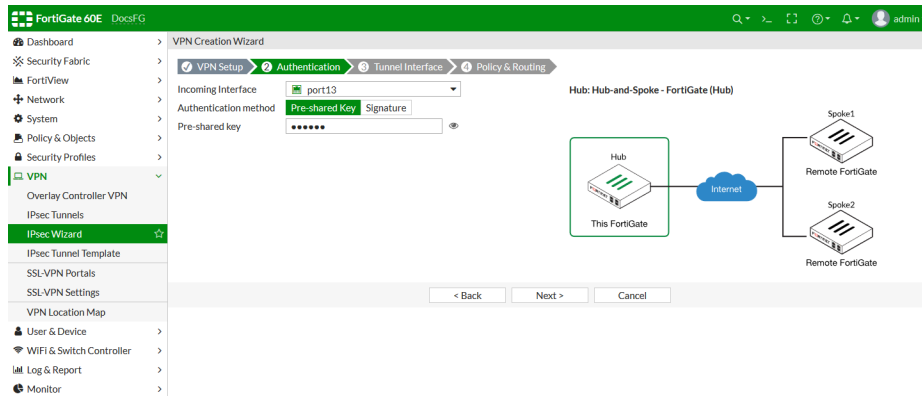
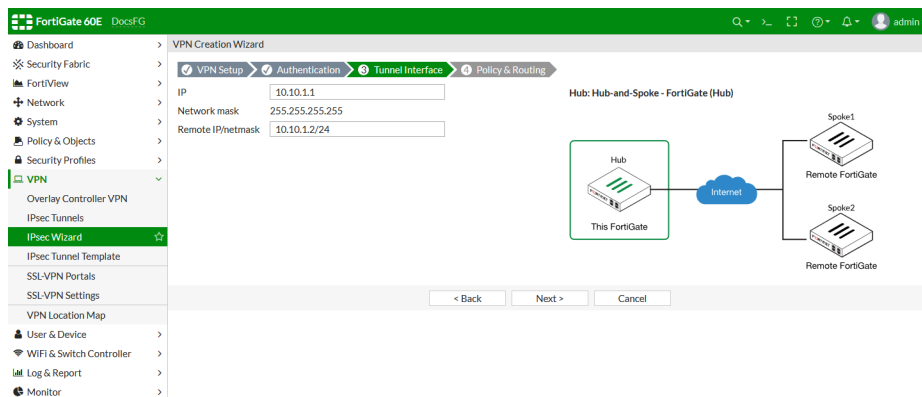
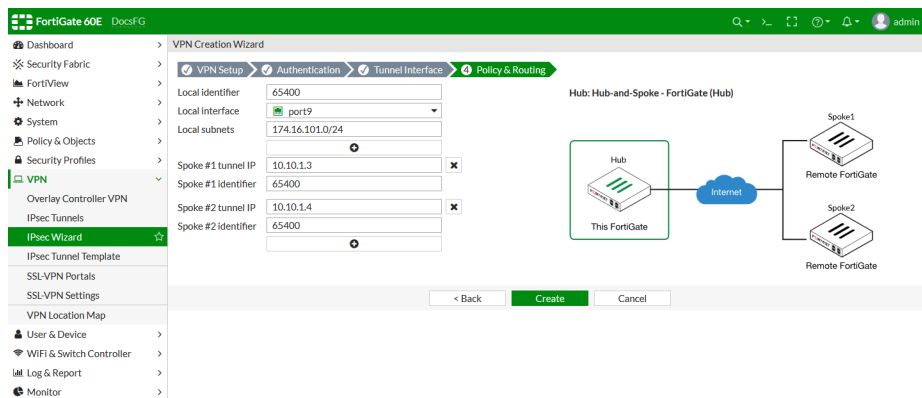
The following example shows the steps in the wizard for configuring a hub and a spoke.

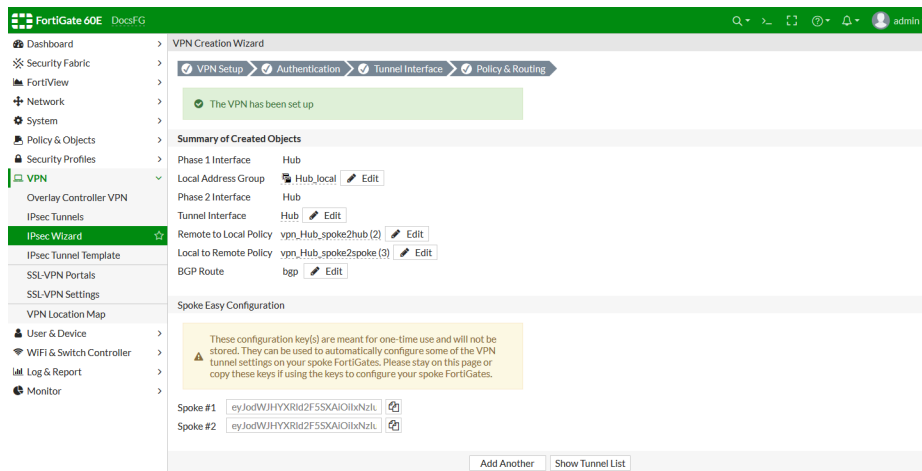
### To configure the hub:

1. On the hub FortiGate, go to *VPN > IPsec Wizard*.



2. Enter a name, set the *Template Type* to *Hub-and-Spoke*, and set the *Role* to *Hub*.

3. Click *Next*.4. Select the *Incoming Interface* and configure the *Authentication method*.5. Click *Next*.6. Set the *IP* address and *Remote IP/netmask*.7. Click *Next*.8. Configure the *Local identifier*, *Local interface*, and *Local subnets*, then configure the tunnel IP addresses and identifiers for the spokes.

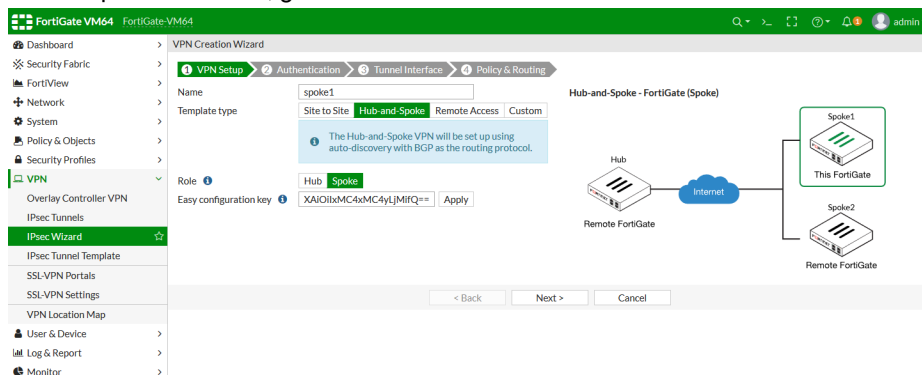
9. Click *Create*.

10. Review the summary to ensure that everything looks as expected.

11. Copy the spokes' easy configuration keys to a temporary location for use when configuring the spokes.

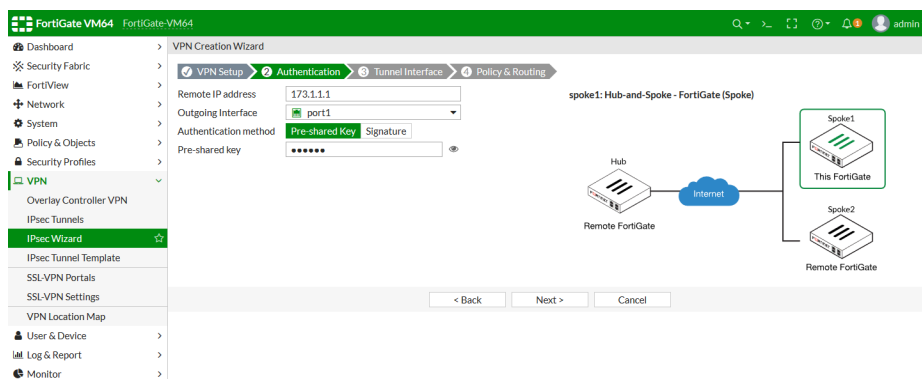
### To configure a spoke:

1. On the spoke FortiGate, go to *VPN > IPsec Wizard*.



2. Enter a name, set the *Template Type* to *Hub-and-Spoke*, set the *Role* to *Spoke*, and paste in the requisite *Easy configuration key* that you saved when configuring the hub.

3. Click *Next*.



4. Set the *Remote IP address*, select the *Incoming Interface*, and configure the *Authentication method*.

5. Click *Next*.

6. Set the *IP* address and *Remote IP/netmask*.7. Click *Next*.

8. Configure the *Local identifier*, *Local interface*, and *Local subnets*, then configure the IP address and identifier of the hub FortiGate.9. Click *Create*.

Summary of Created Objects	
Phase 1 Interface	spoke1
Local Address Group	spoke1_local
Phase 2 Interface	spoke1
Tunnel Interface	spoke1
Remote to Local Policy	vpn_spoke1_remote (1)
Local to Remote Policy	vpn_spoke1_local (2)
BGP Route	bgp

## 10. Review the summary to ensure that everything looks as expected.

## To check the ADVPN shortcut with the IPsec monitor:

1. On either the hub or spoke FortiGate, go to *Monitor > IPsec Monitor*.

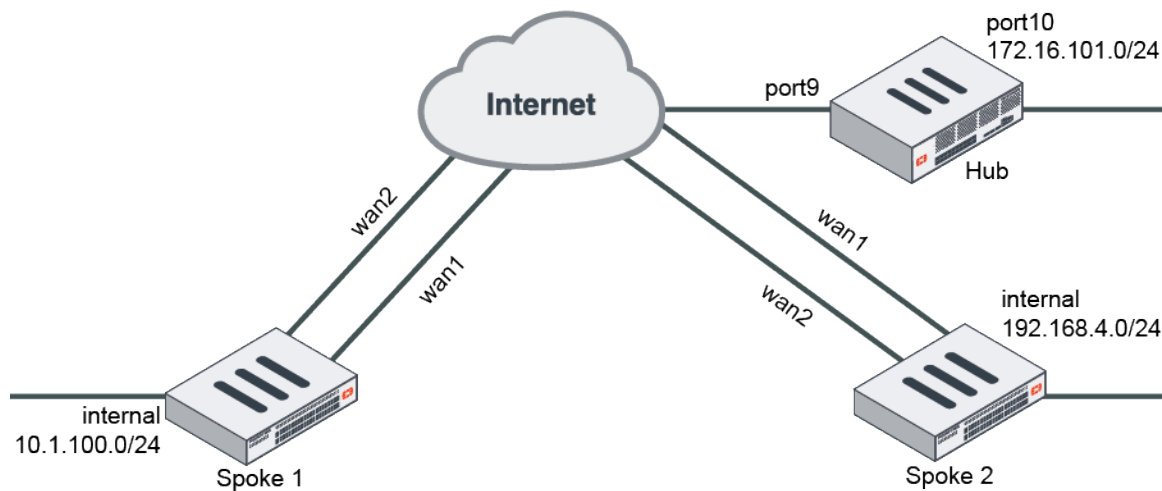
Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Hub-and-Spoke - FortiGate Spoke1						
spoke1	173.1.1.1		32.29 kB	17.27 kB	spoke1	spoke1
spoke1_0	172.16.200.3		2.43 kB	1.34 kB	spoke1_0	spoke1

2 | Updated: 15:03:27

## ADVPN with BGP as the routing protocol

This is a sample configuration of ADVPN with BGP as the routing protocol. The following options must be enabled for this configuration:

- On the hub FortiGate, IPsec phase1-interface `net-device disable` must be run.
- IBGP must be used between the hub and spoke FortiGates.
- `bgp neighbor-group/neighbor-range` must be reused.



Because the GUI can only complete part of the configuration, we recommend using the CLI.

## To configure ADVPN with BGP as the routing protocol using the CLI:

1. Configure hub FortiGate's WAN, internal interface, and static route.

```
config system interface
 edit "port9"
 set alias "WAN"
 set ip 22.1.1.1 255.255.255.0
 next
 edit "port10"
 set alias "Internal"
 set ip 172.16.101.1 255.255.255.0
```



```
 next
 end
 config router static
 edit 1
 set gateway 22.1.1.2
 set device "port9"
 next
 end
```

## 2. Configure the hub FortiGate.

### a. Configure the hub FortiGate IPsec phase1-interface and phase2-interface.

```
config vpn ipsec phase1-interface
 edit "advpn-hub"
 set type dynamic
 set interface "port9"
 set peertype any
 set net-device disable
 set proposal aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1
3des-sha1
 set add-route disable
 set dpd on-idle
 set auto-discovery-sender enable
 set tunnel-search nexthop
 set psksecret sample
 set dpd-retryinterval 5
 next
end
config vpn ipsec phase2-interface
 edit "advpn-hub"
 set phase1name "advpn-hub"
 set proposal aes128-sha1 aes256-sha1 3des-sha1 aes128-sha256 aes256-sha256
3des-sha256
 next
end
```

### b. Configure the hub FortiGate firewall policy.

```
config firewall policy
 edit 1
 set name "spoke2hub"
 set srcintf "advpn-hub"
 set dstintf "port10"
 set srcaddr "all"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set name "spoke2spoke"
 set srcintf "advpn-hub"
 set dstintf "advpn-hub"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
```

```
 set service "ALL"
 next
end
```

**c. Configure the hub FortiGate's IPsec tunnel interface IP address.**

```
config system interface
 edit "advpn-hub1"
 set ip 10.10.10.254 255.255.255.255
 set remote-ip 10.10.10.253 255.255.255.0
 next
end
```

**d. Configure the hub FortiGate's BGP.**

```
config router bgp
 set as 65412
 config neighbor-group
 edit "advpn"
 set link-down-failover enable
 set remote-as 65412
 set route-reflector-client enable
 next
 end
 config neighbor-range
 edit 1
 set prefix 10.10.10.0 255.255.255.0
 set neighbor-group "advpn"
 next
 end
 config network
 edit 1
 set prefix 172.16.101.0 255.255.255.0
 next
 end
end
```

**3. Configure the spoke FortiGates.**

**a. Configure the spoke FortiGates' WAN, internal interfaces, and static routes.**

**i. Configure Spoke1.**

```
config system interface
 edit "wan1"
 set alias "primary_WAN"
 set ip 15.1.1.2 255.255.255.0
 next
 edit "wan2"
 set alias "secondary_WAN"
 set ip 12.1.1.2 255.255.255.0
 next
 edit "internal"
 set ip 10.1.100.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 12.1.1.1
 set device "wan2"
```

```
 set distance 15
 next
 edit 2
 set gateway 15.1.1.1
 set device "wan1"
 next
end
```

## ii. Configure the Spoke2.

```
config system interface
 edit "wan1"
 set alias "primary_WAN"
 set ip 13.1.1.2 255.255.255.0
 next
 edit "wan2"
 set alias "secondary_WAN"
 set ip 17.1.1.2 255.255.255.0
 next
 edit "internal"
 set ip 192.168.4.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 17.1.1.1
 set device "wan2"
 set distance 15
 next
 edit 2
 set gateway 13.1.1.1
 set device "wan1"
 next
end
```

## b. Configure the spoke FortiGates' IPsec phase1-interface and phase2-interface.

### i. Configure Spoke1.

```
config vpn ipsec phase1-interface
 edit "spoke1"
 set interface "wan1"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set add-route disable
 set dpd on-idle
 set auto-discovery-receiver enable
 set remote-gw 22.1.1.1
 set psksecret sample
 set dpd-retryinterval 5
 next
 edit "spoke1_backup"
 set interface "wan2"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set add-route disable
 set dpd on-idle
```

```
 set auto-discovery-receiver enable
 set remote-gw 22.1.1.1
 set monitor "spoke1"
 set psksecret sample
 set dpd-retryinterval 5
 next
end
config vpn ipsec phase2-interface
 edit "spoke1"
 set phase1name "spoke1"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256
aes128gcm aes256gcm chacha20poly1305
 set auto-negotiate enable
 next
 edit "spoke1_backup"
 set phase1name "spoke1_backup"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256
aes128gcm aes256gcm chacha20poly1305
 set auto-negotiate enable
 next
end
```

## ii. Configure Spoke2.

```
config vpn ipsec phase1-interface
 edit "spoke2"
 set interface "wan1"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set add-route disable
 set dpd on-idle
 set auto-discovery-receiver enable
 set remote-gw 22.1.1.1
 set psksecret sample
 set dpd-retryinterval 5
 next
 edit "spoke2_backup"
 set interface "wan2"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set add-route disable
 set dpd on-idle
 set auto-discovery-receiver enable
 set remote-gw 22.1.1.1
 set monitor "spoke2"
 set psksecret sample
 set dpd-retryinterval 5
 next
end
config vpn ipsec phase2-interface
 edit "spoke2"
 set phase1name "spoke2"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256
aes128gcm aes256gcm chacha20poly1305
 set auto-negotiate enable
```

```
next
edit "spoke2_backup"
 set phase1name "spoke2_backup"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256
aes128gcm aes256gcm chacha20poly1305
 set auto-negotiate enable
next
end
```

**c. Configure the spoke FortiGates' firewall policies.**

**i. Configure Spoke1.**

```
config firewall policy
edit 1
 set name "outbound_advpn"
 set srcintf "internal"
 set dstintf "spoke1" "spoke1_backup"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
next
edit 2
 set name "inbound_advpn"
 set srcintf "spoke1" "spoke1_backup"
 set dstintf "internal"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
next
end
```

**ii. Configure Spoke2.**

```
config firewall policy
edit 1
 set name "outbound_advpn"
 set srcintf "internal"
 set dstintf "spoke2" "spoke2_backup"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
next
edit 2
 set name "inbound_advpn"
 set srcintf "spoke2" "spoke2_backup"
 set dstintf "internal"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
```

```
 next
end
```

**d. Configure the spoke FortiGates' tunnel interface IP addresses.**

**i. Configure Spoke1.**

```
config system interface
 edit "spoke1"
 set ip 10.10.10.1 255.255.255.255
 set remote-ip 10.10.10.254 255.255.255.0
 next
 edit "spoke1_backup"
 set ip 10.10.10.2 255.255.255.255
 set remote-ip 10.10.10.254 255.255.255.0
 next
end
```

**ii. Configure Spoke2.**

```
config system interface
 edit "spoke2"
 set ip 10.10.10.3 255.255.255.255
 set remote-ip 10.10.10.254 255.255.255.0
 next
 edit "spoke2_backup"
 set ip 10.10.10.4 255.255.255.255
 set remote-ip 10.10.10.254 255.255.255.0
 next
end
```

**e. Configure the spoke FortiGates' BGP.**

**i. Configure Spoke1.**

```
config router bgp
 set as 65412
 config neighbor
 edit "10.10.10.254"
 set advertisement-interval 1
 set link-down-failover enable
 set remote-as 65412
 next
 end
 config network
 edit 1
 set prefix 10.1.100.0 255.255.255.0
 next
 end
end
```

**ii. Configure Spoke2.**

```
config router bgp
 set as 65412
 config neighbor
 edit "10.10.10.254"
 set advertisement-interval 1
 set link-down-failover enable
 set remote-as 65412
 next
 end
end
```

```

end
config network
 edit 1
 set prefix 192.168.4.0 255.255.255.0
 next
end
end

```

**4. Run diagnose and get commands run on Spoke1 to check VPN and BGP states.**

**a. Run the diagnose vpn tunnel list command on Spoke1. The system should return the following:**

```

list all ipsec tunnel in vd 0

name=spoke1 ver=1 serial=2 15.1.1.2:0->22.1.1.1:0
bound_if=7 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu
create_dev frag-rfc accept_traffic=1

proxyid_num=1 child_num=1 refcnt=19 ilast=1 olast=1 ad=r/2
stat: rxp=1 txp=160 rxb=16428 txb=8969
dpd: mode=on-idle on=1 idle=5000ms retry=3 count=0 seqno=628
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=spoke1 proto=0 sa=1 ref=6 serial=1 auto-negotiate adr
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0
 SA: ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=1225/0B replaywin=1024
 seqno=al esn=0 replaywin_lastseq=00000002 itn=0
 life: type=01 bytes=0/0 timeout=2369/2400
 dec: spi=c53a8f5b esp=aes key=16 cbe88682ad896a69290027b6dd8f7162
 ah=sha1 key=20 7bb704b388f83783ac76c2ab0b6c9f7dcf78e93b
 enc: spi=6e3633fc esp=aes key=16 1a0da3f4deed3d16becc9dda57537355
 ah=sha1 key=20 368544044bd9b82592d72476ff93d5055056da8d
 dec:pkts/bytes=1/16364, enc:pkts/bytes=160/19168
 npu_flag=03 npu_rgwy=22.1.1.1 npu_lgwy=15.1.1.2 npu_selid=1 dec_npuid=1 enc_npuid=1

name=spoke1_backup ver=1 serial=1 12.1.1.2:0->22.1.1.1:0
bound_if=6 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu
create_dev frag-rfc accept_traffic=0

proxyid_num=1 child_num=0 refcnt=11 ilast=0 olast=0 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=5000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=spoke1_backup proto=0 sa=0 ref=2 serial=1 auto-negotiate adr
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0

```

**b. Run the get router info bgp summary command on Spoke1. The system should return the following:**

```

BGP router identifier 7.7.7.7, local AS number 65412
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor V AS [[QualityAssurance62/MsgRcvd]]
[[QualityAssurance62/MsgSent]] [[QualityAssurance62/TblVer]] InQ OutQ Up/Down
State/PfxRcd
10.10.10.254 1. 65412 143 142 1. 1. 1.

```

00:24:45

2

Total number of neighbors 1

- c. Run the `get router info routing-table bgp` command on Spoke1. The system should return the following:

```
Routing table for VRF=0
B 172.16.101.0/24 [200/0] via 10.10.10.254, spoke1, 00:23:57
B 192.168.4.0/24 [200/0] via 10.10.10.254, spoke1, 00:22:03
```

- d. Generate traffic between the spokes and check the shortcut tunnel and routing table. Run the `diagnose vpn tunnel list` command on Spoke1. The system should return the following:

```
list all ipsec tunnel in vd 0

name=spoke1 ver=1 serial=2 15.1.1.2:0->22.1.1.1:0
bound_if=7 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu
create_dev frag-rfc accept_traffic=1

proxyid_num=1 child_num=1 refcnt=19 ilast=2 olast=2 ad=r/2
stat: rxp=1 txp=268 rxb=16428 txb=31243
dpd: mode=on-idle on=1 idle=5000ms retry=3 count=0 seqno=714
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=spoke1 proto=0 sa=1 ref=6 serial=1 auto-negotiate adr
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0
 SA: ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=345/0B replaywin=1024
 seqno=10d esn=0 replaywin_lastseq=00000002 itn=0
 life: type=01 bytes=0/0 timeout=2369/2400
 dec: spi=c53a8f5b esp=aes key=16 cbe88682ad896a69290027b6dd8f7162
 ah=sha1 key=20 7bb704b388f83783ac76c2ab0b6c9f7dcf78e93b
 enc: spi=6e3633fc esp=aes key=16 1a0da3f4deed3d16becc9dda57537355
 ah=sha1 key=20 368544044bd9b82592d72476ff93d5055056da8d
 dec:pkts/bytes=1/16364, enc:pkts/bytes=268/48320
 npu_flag=03 npu_rgwy=22.1.1.1 npu_lgwy=15.1.1.2 npu_selid=1 dec_npuid=1 enc_npuid=1

name=spoke1_backup ver=1 serial=1 12.1.1.2:0->22.1.1.1:0
bound_if=6 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu
create_dev frag-rfc accept_traffic=0

proxyid_num=1 child_num=0 refcnt=11 ilast=8 olast=8 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=5000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=spoke1_backup proto=0 sa=0 ref=2 serial=1 auto-negotiate adr
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0

name=spoke1_0 ver=1 serial=9 15.1.1.2:4500->13.1.1.2:4500
bound_if=7 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/728 options[02d8]=npu
create_dev no-sysctl rgwy-chg frag-rfc accept_traffic=1

parent=spoke1 index=0
proxyid_num=1 child_num=0 refcnt=17 ilast=4 olast=4 ad=r/2
stat: rxp=1 txp=100 rxb=112 txb=4686
dpd: mode=on-idle on=1 idle=5000ms retry=3 count=0 seqno=231
natt: mode=keepalive draft=32 interval=10 remote_port=4500
```



```

proxyid=spoke1 proto=0 sa=1 ref=5 serial=1 auto-negotiate adr
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=6 options=1a227 type=00 soft=0 mtu=1422 expire=447/0B replaywin=1024
seqno=65 esn=0 replaywin_lastseq=00000002 itn=0
life: type=01 bytes=0/0 timeout=2368/2400
dec: spi=c53a8f5c esp=aes key=16 73fd9869547475db78851e6c057ad9b7
ah=sha1 key=20 6ad3a5b1028f6b33c82ba494a370f13c7f462635
enc: spi=79cb0f2b esp=aes key=16 52ab0acdc830d58c00e5956a6484654a
ah=sha1 key=20 baa82aba4106dc60618f6fe95570728656799239
dec:pkts/bytes=1/46, enc:pkts/bytes=100/11568
npu_flag=03 npu_rgw=13.1.1.2 npu_lgw=15.1.1.2 npu_selid=5 dec_npuid=1 enc_npuid=1

```

- e. Run the `get router info routing-table bgp` command. The system should return the following:

```

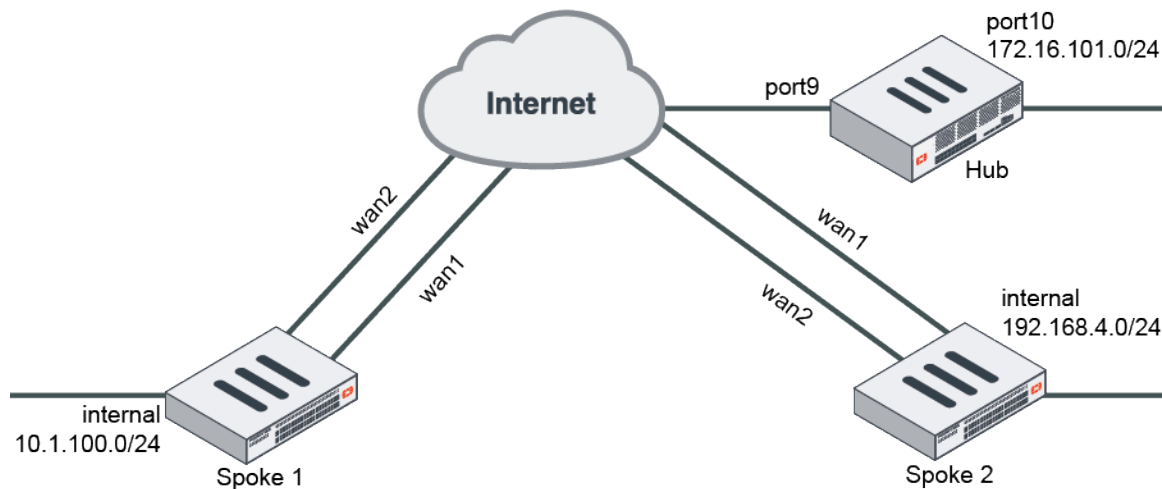
Routing table for VRF=0
B 172.16.101.0/24 [200/0] via 10.10.10.254, spoke1, 00:23:57
B 192.168.4.0/24 [200/0] via 10.10.10.3, spoke1_0 , 00:22:03

```

## ADVPN with OSPF as the routing protocol

This is a sample configuration of ADVPN with OSPF as the routing protocol. The following options must be enabled for this configuration:

- On the hub FortiGate, IPsec phase1-interface `net-device enable` must be run.
- OSPF must be used between the hub and spoke FortiGates.



Because the GUI can only complete part of the configuration, we recommend using the CLI.

### To configure ADVPN with OSPF as the routing protocol using the CLI:

1. Configure hub FortiGate's WAN, internal interface, and static route.

```

config system interface
edit "port9"
set alias "WAN"
set ip 22.1.1.1 255.255.255.0
next
edit "port10"

```

```
 set alias "Internal"
 set ip 172.16.101.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 22.1.1.2
 set device "port9"
 next
end
```

## 2. Configure the hub FortiGate.

### a. Configure the hub FortiGate IPsec phase1-interface and phase2-interface.

```
config vpn ipsec phase1-interface
 edit "advpn-hub"
 set type dynamic
 set interface "port9"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1
3des-sha1
 set add-route disable
 set dpd on-idle
 set auto-discovery-sender enable
 set tunnel-search nexthop
 set psksecret sample
 set dpd-retryinterval 5
 next
end
config vpn ipsec phase2-interface
 edit "advpn-hub"
 set phase1name "advpn-hub"
 set proposal aes128-sha1 aes256-sha1 3des-sha1 aes128-sha256 aes256-sha256
3des-sha256
 next
end
```

### b. Configure the hub FortiGate firewall policy.

```
config firewall policy
 edit 1
 set name "spoke2hub"
 set srcintf "advpn-hub"
 set dstintf "port10"
 set srcaddr "all"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set name "spoke2spoke"
 set srcintf "advpn-hub"
 set dstintf "advpn-hub"
 set srcaddr "all"
 set dstaddr "all"
```

```

 set action accept
 set schedule "always"
 set service "ALL"
 next
end

```

**c. Configure the hub FortiGate's IPsec tunnel interface IP address.**

```

config system interface
 edit "advpn-hub1"
 set ip 10.10.10.254 255.255.255.255
 set remote-ip 10.10.10.253 255.255.255.0
 next
end

```

**d. Configure the hub FortiGate's OSPF.**

```

config router ospf
 set router-id 1.1.1.1
 config area
 edit 0.0.0.0
 next
 end
 config network
 edit 1
 set prefix 10.10.10.0 255.255.255.0
 next
 edit 2
 set prefix 172.16.101.0 255.255.255.0
 next
 end
end

```

**3. Configure the spoke FortiGates.**

**a. Configure the spoke FortiGates' WAN, internal interfaces, and static routes.**

**i. Configure Spoke1.**

```

config system interface
 edit "wan1"
 set alias "primary_WAN"
 set ip 15.1.1.2 255.255.255.0
 next
 edit "wan2"
 set alias "secondary_WAN"
 set ip 12.1.1.2 255.255.255.0
 next
 edit "internal"
 set ip 10.1.100.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 12.1.1.1
 set device "wan2"
 set distance 15
 next
 edit 2
 set gateway 15.1.1.1

```

```

 set device "wan1"
 next
end

```

## ii. Configure the Spoke2.

```

config system interface
 edit "wan1"
 set alias "primary_WAN"
 set ip 13.1.1.2 255.255.255.0
 next
 edit "wan2"
 set alias "secondary_WAN"
 set ip 17.1.1.2 255.255.255.0
 next
 edit "internal"
 set ip 192.168.4.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 17.1.1.1
 set device "wan2"
 set distance 15
 next
 edit 2
 set gateway 13.1.1.1
 set device "wan1"
 next
end

```

## b. Configure the spoke FortiGates' IPsec phase1-interface and phase2-interface.

### i. Configure Spoke1.

```

config vpn ipsec phase1-interface
 edit "spoke1"
 set interface "wan1"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set add-route disable
 set dpd on-idle
 set auto-discovery-receiver enable
 set remote-gw 22.1.1.1
 set psksecret sample
 set dpd-retryinterval 5
 next
 edit "spoke1_backup"
 set interface "wan2"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set add-route disable
 set dpd on-idle
 set auto-discovery-receiver enable
 set remote-gw 22.1.1.1
 set monitor "spoke1"
 set psksecret sample
 next
end

```

```

 set dpd-retryinterval 5
 next
end
config vpn ipsec phase2-interface
 edit "spoke1"
 set phase1name "spoke1"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256
aes128gcm aes256gcm chacha20poly1305
 set auto-negotiate enable
 next
 edit "spoke1_backup"
 set phase1name "spoke1_backup"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256
aes128gcm aes256gcm chacha20poly1305
 set auto-negotiate enable
 next
end

```

## ii. Configure Spoke2.

```

config vpn ipsec phase1-interface
 edit "spoke2"
 set interface "wan1"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set add-route disable
 set dpd on-idle
 set auto-discovery-receiver enable
 set remote-gw 22.1.1.1
 set psksecret sample
 set dpd-retryinterval 5
 next
 edit "spoke2_backup"
 set interface "wan2"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set add-route disable
 set dpd on-idle
 set auto-discovery-receiver enable
 set remote-gw 22.1.1.1
 set monitor "spoke2"
 set psksecret sample
 set dpd-retryinterval 5
 next
end
config vpn ipsec phase2-interface
 edit "spoke2"
 set phase1name "spoke2"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256
aes128gcm aes256gcm chacha20poly1305
 set auto-negotiate enable
 next
 edit "spoke2_backup"
 set phase1name "spoke2_backup"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256

```

```
 aes128gcm aes256gcm chacha20poly1305
 set auto-negotiate enable
 next
end
```

**c. Configure the spoke FortiGates' firewall policies.**

**i. Configure Spoke1.**

```
config firewall policy
 edit 1
 set name "outbound_advpn"
 set srcintf "internal"
 set dstintf "spoke1" "spoke1_backup"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set name "inbound_advpn"
 set srcintf "spoke1" "spoke1_backup"
 set dstintf "internal"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end
```

**ii. Configure Spoke2.**

```
config firewall policy
 edit 1
 set name "outbound_advpn"
 set srcintf "internal"
 set dstintf "spoke2" "spoke2_backup"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set name "inbound_advpn"
 set srcintf "spoke2" "spoke2_backup"
 set dstintf "internal"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end
```

**d. Configure the spoke FortiGates' tunnel interface IP addresses.****i. Configure Spoke1.**

```
config system interface
 edit "spoke1"
 set ip 10.10.10.1 255.255.255.255
 set remote-ip 10.10.10.254 255.255.255.0
 next
 edit "spoke1_backup"
 set ip 10.10.10.2 255.255.255.255
 set remote-ip 10.10.10.254 255.255.255.0
 next
end
```

**ii. Configure Spoke2.**

```
config system interface
 edit "spoke2"
 set ip 10.10.10.3 255.255.255.255
 set remote-ip 10.10.10.254 255.255.255.0
 next
 edit "spoke2_backup"
 set ip 10.10.10.4 255.255.255.255
 set remote-ip 10.10.10.254 255.255.255.0
 next
end
```

**e. Configure the spoke FortiGates' OSPF.****i. Configure Spoke1.**

```
config router ospf
 set router-id 7.7.7.7
 config area
 edit 0.0.0.0
 next
end
config network
 edit 1
 set prefix 10.10.10.0 255.255.255.0
 next
 edit 2
 set prefix 10.1.100.0 255.255.255.0
 next
end
end
```

**ii. Configure Spoke2.**

```
config router ospf
 set router-id 8.8.8.8
 config area
 edit 0.0.0.0
 next
end
config network
 edit 1
 set prefix 10.10.10.0 255.255.255.0
 next
 edit 2
```

```

 set prefix 192.168.4.0 255.255.255.0
 next
end
end

```

**4. Run diagnose and get commands on Spoke1 to check VPN and OSPF states.**

**a. Run the diagnose vpn tunnel list command on Spoke1. The system should return the following:**

```

list all ipsec tunnel in vd 0

name=spoke1 ver=1 serial=2 15.1.1.2:0->22.1.1.1:0
bound_if=7 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu
create_dev frag-rfc accept_traffic=1

proxyid_num=1 child_num=1 refcnt=19 ilast=5 olast=2 ad=r/2
stat: rxp=1 txp=263 rxb=16452 txb=32854
dpd: mode=on-idle on=1 idle=5000ms retry=3 count=0 seqno=2283
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=spoke1 proto=0 sa=1 ref=5 serial=1 auto-negotiate adr
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0
 SA: ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=1057/0B replaywin=1024
 seqno=108 esn=0 replaywin_lastseq=00000003 itn=0
 life: type=01 bytes=0/0 timeout=2371/2400
 dec: spi=c53a8f78 esp=aes key=16 7cc50c5c9df1751f6497a4ad764c5e9a
 ah=sha1 key=20 269292ddbf7309a6fc05871e63ed8a5297b5c9a1
 enc: spi=6e363612 esp=aes key=16 42bd49bcd1e85cf74a24d97f10eb601
 ah=sha1 key=20 13964f166aad48790c2e551d6df165d7489f524b
 dec:pkts/bytes=1/16394, enc:pkts/bytes=263/50096
 npu_flag=03 npu_rgwy=22.1.1.1 npu_lgwy=15.1.1.2 npu_selid=1 dec_npuid=1 enc_npuid=1

name=spoke1_backup ver=1 serial=1 12.1.1.2:0->22.1.1.1:0
bound_if=6 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu
create_dev frag-rfc accept_traffic=0

proxyid_num=1 child_num=0 refcnt=11 ilast=8 olast=8 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=5000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=spoke1_backup proto=0 sa=0 ref=2 serial=1 auto-negotiate adr
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0

```

**b. Run the get router info ospf neighbor command on Spoke1. The system should return the following:**

```

OSPF process 0, VRF 0: Neighbor ID Pri State Dead Time Address Interface 8.8.8.8 1.
Full/ - 00:00:35 10.10.10.254 spoke1 1.1.1.1 1. Full/ - 00:00:35 10.10.10.254 spoke1

```

**c. Run the get router info routing-table ospf command on Spoke1. The system should return the following:**

```

Routing table for VRF=0
O 172.16.101.0/24 [110/110] via 10.10.10.254, spoke1, 00:23:23
O 192.168.4.0/24 [110/110] via 10.10.10.254, spoke1, 00:22:35

```

**d. Generate traffic between the spokes, then check the shortcut tunnel and routing table. Run the diagnose vpn tunnel list command on Spoke1. The system should return the following:**



```

list all ipsec tunnel in vd 0

name=spokel ver=1 serial=2 15.1.1.2:0->22.1.1.1:0
bound_if=7 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu
create_dev frag-rfc accept_traffic=1

proxyid_num=1 child_num=1 refcnt=19 ilast=2 olast=2 ad=r/2
stat: rxp=1 txp=313 rxb=16452 txb=35912
dpd: mode=on-idle on=1 idle=5000ms retry=3 count=0 seqno=2303
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=spokel proto=0 sa=1 ref=3 serial=1 auto-negotiate adr
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0
 SA: ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=782/0B replaywin=1024
 seqno=13a esn=0 replaywin_lastseq=00000003 itn=0
 life: type=01 bytes=0/0 timeout=2371/2400
 dec: spi=c53a8f78 esp=aes key=16 7cc50c5c9df1751f6497a4ad764c5e9a
 ah=sha1 key=20 269292ddb7f7309a6fc05871e63ed8a5297b5c9a1
 enc: spi=6e363612 esp=aes key=16 42bd49bcd1e85cf74a24d97f10eb601
 ah=sha1 key=20 13964f166aad48790c2e551d6df165d7489f524b
 dec:pkts/bytes=1/16394, enc:pkts/bytes=313/56432
 npu_flag=03 npu_rgw=22.1.1.1 npu_lgw=15.1.1.2 npu_selid=1 dec_npuid=1 enc_npuid=1

name=spokel_backup ver=1 serial=1 12.1.1.2:0->22.1.1.1:0
bound_if=6 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu
create_dev frag-rfc accept_traffic=0

proxyid_num=1 child_num=0 refcnt=11 ilast=13 olast=13 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=5000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=spokel_backup proto=0 sa=0 ref=2 serial=1 auto-negotiate adr
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0

name=spokel_0 ver=1 serial=e 15.1.1.2:4500->13.1.1.2:4500
bound_if=7 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/728 options[02d8]=npu
create_dev no-sysctl rgwy-chg frag-rfc accept_traffic=1

parent=spokel index=0
proxyid_num=1 child_num=0 refcnt=19 ilast=4 olast=2 ad=r/2
stat: rxp=641 txp=1254 rxb=278648 txb=161536
dpd: mode=on-idle on=1 idle=5000ms retry=3 count=0 seqno=184
natt: mode=keepalive draft=32 interval=10 remote_port=4500
proxyid=spokel_backup proto=0 sa=1 ref=10 serial=1 auto-negotiate adr
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0
 SA: ref=6 options=1a227 type=00 soft=0 mtu=1422 expire=922/0B replaywin=1024
 seqno=452 esn=0 replaywin_lastseq=00000280 itn=0
 life: type=01 bytes=0/0 timeout=2370/2400
 dec: spi=c53a8f79 esp=aes key=16 324f8cf840ba6722cc7abbba46b34e0e
 ah=sha1 key=20 a40e9aac596b95c4cd83a7f6372916a5ef5aa505
 enc: spi=ef3327b5 esp=aes key=16 5909d6066b303de4520d2b5ae2db1b61
 ah=sha1 key=20 1a42f5625b5a335d8d5282fe83b5d6c6ff26b2a4

```

```
dec:pkts/bytes=641/278568, enc:pkts/bytes=1254/178586
npu_flag=03 npu_rgw=13.1.1.2 npu_lgw=15.1.1.2 npu_selid=a dec_npuid=1 enc_npuid=1
```

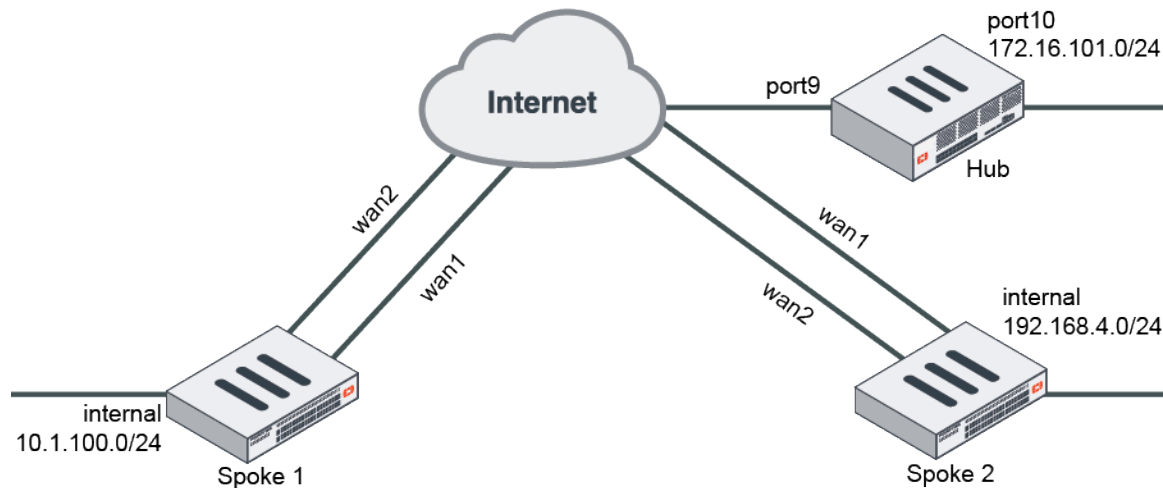
- e. Run the `get router info routing-table ospf` command. The system should return the following:

```
Routing table for VRF=0
O 172.16.101.0/24 [110/110] via 10.10.10.254, spoke1, 00:27:14
O 192.168.4.0/24 [110/110] via 10.10.10.3, spoke1_0, 00:26:26
```

## ADVPN with RIP as the routing protocol

This is a sample configuration of ADVPN with RIP as routing protocol. The following options must be enabled for this configuration:

- On the hub FortiGate, IPsec phase1-interface `net-device disable` must be run.
- RIP must be used between the hub and spoke FortiGates.
- `split-horizon-status enable` must be run on the hub FortiGate.



Because the GUI can only complete part of the configuration, we recommend using the CLI.

### To configure ADVPN with RIP as the routing protocol using the CLI:

1. In the CLI, configure hub FortiGate's WAN, internal interface, and static route.

```
config system interface
 edit "port9"
 set alias "WAN"
 set ip 22.1.1.1 255.255.255.0
 next
 edit "port10"
 set alias "Internal"
 set ip 172.16.101.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 22.1.1.2
 set device "port9"
```

```
 next
end
```

## 2. Configure the hub FortiGate.

### a. Configure the hub FortiGate IPsec phase1-interface and phase2-interface.

```
config vpn ipsec phase1-interface
 edit "advpn-hub"
 set type dynamic
 set interface "port9"
 set peertype any
 set net-device disable
 set proposal aes128-sha256 aes256-sha256 3des-sha256 aes128-sha1 aes256-sha1
3des-sha1
 set add-route disable
 set dpd on-idle
 set auto-discovery-sender enable
 set tunnel-search nexthop
 set psksecret sample
 set dpd-retryinterval 5
 next
end
config vpn ipsec phase2-interface
 edit "advpn-hub"
 set phase1name "advpn-hub"
 set proposal aes128-sha1 aes256-sha1 3des-sha1 aes128-sha256 aes256-sha256
3des-sha256
 next
end
```

### b. Configure the hub FortiGate firewall policy.

```
config firewall policy
 edit 1
 set name "spoke2hub"
 set srcintf "advpn-hub"
 set dstintf "port10"
 set srcaddr "all"
 set dstaddr "172.16.101.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set name "spoke2spoke"
 set srcintf "advpn-hub"
 set dstintf "advpn-hub"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end
```

**c. Configure the hub FortiGate's IPsec tunnel interface IP address.**

```
config system interface
 edit "advpn-hub1"
 set ip 10.10.10.254 255.255.255.255
 set remote-ip 10.10.10.253 255.255.255.0
 next
end
```

**d. Configure the hub FortiGate's RIP.**

```
config router rip
 set default-information-originate enable
 config network
 edit 1
 set prefix 10.10.10.0 255.255.255.0
 next
 edit 2
 set prefix 172.16.101.0 255.255.255.0
 next
 end
 config interface
 edit "advpn-hub"
 set split-horizon-status disable
 next
 end
end
```

**3. Configure the spoke FortiGates.****a. Configure the spoke FortiGates' WAN, internal interfaces, and static routes.****i. Configure Spoke1.**

```
config system interface
 edit "wan1"
 set alias "primary_WAN"
 set ip 15.1.1.2 255.255.255.0
 next
 edit "wan2"
 set alias "secondary_WAN"
 set ip 12.1.1.2 255.255.255.0
 next
 edit "internal"
 set ip 10.1.100.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 12.1.1.1
 set device "wan2"
 set distance 15
 next
 edit 2
 set gateway 15.1.1.1
 set device "wan1"
 next
end
```

**ii. Configure the Spoke2.**

```
config system interface
 edit "wan1"
 set alias "primary_WAN"
 set ip 13.1.1.2 255.255.255.0
 next
 edit "wan2"
 set alias "secondary_WAN"
 set ip 17.1.1.2 255.255.255.0
 next
 edit "internal"
 set ip 192.168.4.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 17.1.1.1
 set device "wan2"
 set distance 15
 next
 edit 2
 set gateway 13.1.1.1
 set device "wan1"
 next
end
```

**b. Configure the spoke FortiGates' IPsec phase1-interface and phase2-interface.****i. Configure Spoke1.**

```
config vpn ipsec phase1-interface
 edit "spoke1"
 set interface "wan1"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set add-route disable
 set dpd on-idle
 set auto-discovery-receiver enable
 set remote-gw 22.1.1.1
 set psksecret sample
 set dpd-retryinterval 5
 next
 edit "spoke1_backup"
 set interface "wan2"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set add-route disable
 set dpd on-idle
 set auto-discovery-receiver enable
 set remote-gw 22.1.1.1
 set monitor "spoke1"
 set psksecret sample
 set dpd-retryinterval 5
 next
end
```

```
config vpn ipsec phase2-interface
 edit "spoke1"
 set phase1name "spoke1"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256
aes128gcm aes256gcm chacha20poly1305
 set auto-negotiate enable
 next
 edit "spoke1_backup"
 set phase1name "spoke1_backup"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256
aes128gcm aes256gcm chacha20poly1305
 set auto-negotiate enable
 next
end
```

## ii. Configure Spoke2.

```
config vpn ipsec phase1-interface
 edit "spoke2"
 set interface "wan1"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set add-route disable
 set dpd on-idle
 set auto-discovery-receiver enable
 set remote-gw 22.1.1.1
 set psksecret sample
 set dpd-retryinterval 5
 next
 edit "spoke2_backup"
 set interface "wan2"
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set add-route disable
 set dpd on-idle
 set auto-discovery-receiver enable
 set remote-gw 22.1.1.1
 set monitor "spoke2"
 set psksecret sample
 set dpd-retryinterval 5
 next
end
config vpn ipsec phase2-interface
 edit "spoke2"
 set phase1name "spoke2"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256
aes128gcm aes256gcm chacha20poly1305
 set auto-negotiate enable
 next
 edit "spoke2_backup"
 set phase1name "spoke2_backup"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256
aes128gcm aes256gcm chacha20poly1305
 set auto-negotiate enable
```

```
 next
end
```

**c. Configure the spoke FortiGates' firewall policies.**

**i. Configure Spoke1.**

```
config firewall policy
 edit 1
 set name "outbound_advpn"
 set srcintf "internal"
 set dstintf "spoke1" "spoke1_backup"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set name "inbound_advpn"
 set srcintf "spoke1" "spoke1_backup"
 set dstintf "internal"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end
```

**ii. Configure Spoke2.**

```
config firewall policy
 edit 1
 set name "outbound_advpn"
 set srcintf "internal"
 set dstintf "spoke2" "spoke2_backup"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set name "inbound_advpn"
 set srcintf "spoke2" "spoke2_backup"
 set dstintf "internal"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end
```

**d. Configure the spoke FortiGates' tunnel interface IP addresses.****i. Configure Spoke1.**

```
config system interface
 edit "spoke1"
 set ip 10.10.10.1 255.255.255.255
 set remote-ip 10.10.10.254 255.255.255.0
 next
 edit "spoke1_backup"
 set ip 10.10.10.2 255.255.255.255
 set remote-ip 10.10.10.254 255.255.255.0
 next
end
```

**ii. Configure Spoke2.**

```
config system interface
 edit "spoke2"
 set ip 10.10.10.3 255.255.255.255
 set remote-ip 10.10.10.254 255.255.255.0
 next
 edit "spoke2_backup"
 set ip 10.10.10.4 255.255.255.255
 set remote-ip 10.10.10.254 255.255.255.0
 next
end
```

**e. Configure the spoke FortiGates' RIP.****i. Configure Spoke1.**

```
config router rip
 config network
 edit 1
 set prefix 10.10.10.0 255.255.255.0
 next
 edit 2
 set prefix 10.1.100.0 255.255.255.0
 next
 end
end
```

**ii. Configure Spoke2.**

```
config router rip
 config network
 edit 1
 set prefix 10.10.10.0 255.255.255.0
 next
 edit 2
 set prefix 192.168.4.0 255.255.255.0
 next
 end
end
```

**4. Run diagnose and get commands on Spoke1.****a. Run the diagnose vpn tunnel list command on Spoke1. The system should return the following:**

```
list all ipsec tunnel in vd 0

```



```

name=spoke1 ver=1 serial=2 15.1.1.2:0->22.1.1.1:0
bound_if=7 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu
create_dev frag-rfc accept_traffic=1

proxyid_num=1 child_num=1 refcnt=17 ilast=2 olast=2 ad=r/2
stat: rxp=1 txp=87 rxb=200 txb=6208
dpd: mode=on-idle on=1 idle=5000ms retry=3 count=0 seqno=1040
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=spoke1 proto=0 sa=1 ref=4 serial=1 auto-negotiate adr
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0
 SA: ref=7 options=1a227 type=00 soft=0 mtu=1438 expire=1793/0B replaywin=1024
 seqno=57 esn=0 replaywin_lastseq=00000002 itn=0
 life: type=01 bytes=0/0 timeout=2370/2400
 dec: spi=c53a8f60 esp=aes key=16 6b54e32d54d039196a74d96e96d1cf14
 ah=sha1 key=20 e4903474614eafc96eda6400a3a5e88bbcb26a7f
 enc: spi=6e36349d esp=aes key=16 914a40a7993eda75c4dea2f42905f27d
 ah=sha1 key=20 8040eb08342edea2dae5eee058fd054a46688267
 dec:pkts/bytes=1/132, enc:pkts/bytes=86/11696
 npu_flag=03 npu_rgwy=22.1.1.1 npu_lgwy=15.1.1.2 npu_selid=1 dec_npuid=1 enc_npuid=1

name=spoke1_backup ver=1 serial=1 12.1.1.2:0->22.1.1.1:0
bound_if=6 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu
create_dev frag-rfc accept_traffic=0

proxyid_num=1 child_num=0 refcnt=11 ilast=0 olast=0 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=5000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=spoke1_backup proto=0 sa=0 ref=2 serial=1 auto-negotiate adr
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0

```

- b. Run the `get router info rip database` command on Spoke1. The system should return the following:**

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,  
C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP

Network	Next Hop	Metric From	If	Time
Rc 10.1.100.0/24		1.	internal	
Rc 10.10.10.2/32		1.	spoke1	
R 172.16.101.0/24	10.10.10.254	1. 10.10.10.254	spoke1	02:28
R 192.168.4.0/24	10.10.10.254	1. 10.10.10.254	spoke1	02:44

- c. Run the `get router info routing-table rip` command on Spoke1. The system should return the following:**

```

Routing table for VRF=0
R 172.16.101.0/24 [120/2] via 10.10.10.254, spoke1, 00:08:38
R 192.168.4.0/24 [120/3] via 10.10.10.254, spoke1, 00:08:38

```

- d. Generate traffic between the spokes, then check the shortcut tunnel and routing table. Run the `diagnose vpn tunnel list` command on Spoke1. The system should return the following:**

```

list all ipsec tunnel in vd 0

name=spoke1 ver=1 serial=2 15.1.1.2:0->22.1.1.1:0
bound_if=7 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu

```

```

create_dev frag-rfc accept_traffic=1

proxyid_num=1 child_num=0 refcnt=19 ilast=3 olast=3 ad=r/2
stat: rxp=1 txp=78 rxb=200 txb=5546
dpd: mode=on-idle on=1 idle=5000ms retry=3 count=0 seqno=1039
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=spokel proto=0 sa=1 ref=5 serial=1 auto-negotiate adr
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0
 SA: ref=7 options=1a227 type=00 soft=0 mtu=1438 expire=1807/0B replaywin=1024
 seqno=4e esn=0 replaywin_lastseq=00000002 itn=0
 life: type=01 bytes=0/0 timeout=2370/2400
 dec: spi=c53a8f60 esp=aes key=16 6b54e32d54d039196a74d96e96d1cf14
 ah=shal key=20 e4903474614eafc96eda6400a3a5e88bbcb26a7f
 enc: spi=6e36349d esp=aes key=16 914a40a7993eda75c4dea2f42905f27d
 ah=shal key=20 8040eb08342edea2dae5eee058fd054a46688267
 dec:pkts/bytes=1/132, enc:pkts/bytes=77/10456
 npu_flag=03 npu_rgw=22.1.1.1 npu_lgw=15.1.1.2 npu_selid=1 dec_npuid=1 enc_npuid=1

name=spokel_backup ver=1 serial=1 12.1.1.2:0->22.1.1.1:0
bound_if=6 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/536 options[0218]=npu
create_dev frag-rfc accept_traffic=0

proxyid_num=1 child_num=0 refcnt=11 ilast=20 olast=20 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=5000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=spokel_backup proto=0 sa=0 ref=2 serial=1 auto-negotiate adr
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0

name=spokel_0 ver=1 serial=a 15.1.1.2:4500->13.1.1.2:4500
bound_if=7 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/728 options[02d8]=npu
create_dev no-sysctl rgwy-chg frag-rfc accept_traffic=1

parent=spokel index=0
proxyid_num=1 child_num=0 refcnt=20 ilast=2 olast=0 ad=r/2
stat: rxp=1 txp=7 rxb=112 txb=480
dpd: mode=on-idle on=1 idle=5000ms retry=3 count=0 seqno=0
natt: mode=keepalive draft=32 interval=10 remote_port=4500
proxyid=spokel proto=0 sa=1 ref=8 serial=1 auto-negotiate adr
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0
 SA: ref=6 options=1a227 type=00 soft=0 mtu=1422 expire=2358/0B replaywin=1024
 seqno=8 esn=0 replaywin_lastseq=00000002 itn=0
 life: type=01 bytes=0/0 timeout=2367/2400
 dec: spi=c53a8f61 esp=aes key=16 c66aa7ae9657068108ed47c048ff56b6
 ah=shal key=20 60661c68e20bbc913c2564ade85e01ea3769e703
 enc: spi=79cb0f30 esp=aes key=16 bf6c898c2e1c64baaa679ed5d79c3b58
 ah=shal key=20 146ca78be6c34eedb9cd66cc328216e08682ecb1
 dec:pkts/bytes=1/46, enc:pkts/bytes=7/992
 npu_flag=03 npu_rgw=13.1.1.2 npu_lgw=15.1.1.2 npu_selid=6 dec_npuid=1 enc_npuid=1

```

- e. Run the `get router info routing-table rip` command. The system should return the following:

```

Routing table for VRF=0
R 172.16.101.0/24 [120/2] via 10.10.10.254, spoke1, 00:09:04
R 192.168.4.0/24 [120/2] via 10.10.10.3, spoke1_0, 00:00:02

```

## Other VPN topics

The following topics provide instructions on configuring other VPN topics.

- [VPN and ASIC offload on page 1341](#)
- [Encryption algorithms on page 1351](#)
- [Fragmenting IP packets before IPsec encapsulation on page 1358](#)
- [VXLAN over IPsec tunnel on page 1359](#)

## VPN and ASIC offload

This topic provides a brief introduction to VPN traffic offloading.

### IPsec traffic processed by NPU

1. Check the device ASIC information. For example, a FortiGate 900D has an NP6 and a CP8.

```

get hardware status
Model name: [[QualityAssurance62/FortiGate]]-900D
ASIC version: CP8
ASIC SRAM: 64M
CPU: Intel(R) Xeon(R) CPU E3-1225 v3 @ 3.20GHz
Number of CPUs: 4
RAM: 16065 MB
Compact Flash: 1925 MB /dev/sda
Hard disk: 244198 MB /dev/sdb
USB Flash: not available
Network Card chipset: [[QualityAssurance62/FortiASIC]] NP6 Adapter (rev.)

```

2. Check port to NPU mapping.

```

diagnose npu np6 port-list
Chip XAUI Ports Max Cross-chip
 Speed offloading

np6_0 0
 1. port17 1G Yes
 1. port18 1G Yes
 1. port19 1G Yes
 1. port20 1G Yes
 1. port21 1G Yes
 1. port22 1G Yes
 1. port23 1G Yes
 1. port24 1G Yes
 1. port27 1G Yes
 1. port28 1G Yes
 1. port25 1G Yes
 1. port26 1G Yes
 1. port31 1G Yes

```

```

1. port32 1G Yes
1. port29 1G Yes
1. port30 1G Yes
1. portB 10G Yes
1.

np6_1 0
1. port1 1G Yes
1. port2 1G Yes
1. port3 1G Yes
1. port4 1G Yes
1. port5 1G Yes
1. port6 1G Yes
1. port7 1G Yes
1. port8 1G Yes
1. port11 1G Yes
1. port12 1G Yes
1. port9 1G Yes
1. port10 1G Yes
1. port15 1G Yes
1. port16 1G Yes
1. port13 1G Yes
1. port14 1G Yes
1. portA 10G Yes
1.

```

3. Configure the option in IPsec phase1 settings to control NPU encrypt/decrypt IPsec packets (enabled by default).

```

config vpn ipsec phase1/phase1-interface
 edit "vpn_name"
 set npu-offload enable/disable
 next
end

```

4. Check NPU offloading. The NPU encrypted/decrypted counter should tick. The `npu_flag 03` flag means that the traffic processed by the NPU is bi-directional.

```

diagnose vpn tunnel list
list all ipsec tunnel in vd 0

name=test ver=2 serial=1 173.1.1.1:0->11.101.1.1:0
bound_if=42 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/8 options[0008]=npu
proxyid_num=1 child_num=0 refcnt=14 ilast=2 olast=2 ad=/0
stat: rxp=12231 txp=12617 rxb=1316052 txb=674314
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=test proto=0 sa=1 ref=4 serial=7
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=6 options=10626 type=00 soft=0 mtu=1438 expire=42921/0B replaywin=2048
seqno=802 esn=0 replaywin_lastseq=00000680 itn=0
life: type=01 bytes=0/0 timeout=42930/43200
dec: spi=e313ac46 esp=aes key=16 0dcb52642eed18b852b5c65a7dc62958
 ah=md5 key=16 c61d9fe60242b9a30e60b1d01da77660
enc: spi=706ffe03 esp=aes key=16 6ad98c204fa70545dbf3d2e33fb7b529
 ah=md5 key=16 dcc3b866da155ef73c0aba15ec530e2e

```

```
dec:pkts/bytes=1665/16352, enc:pkts/bytes=2051/16826
npu_flag=03 npu_rgwy=11.101.1.1 npu_lgwy=173.1.1.1 npu_selid=6 dec_npuid=2 enc_npuid=2
```

```
FGT_900D # diagnose vpn ipsec st
```

```
All ipsec crypto devices in use:
```

```
NP6_0:
```

```
Encryption (encrypted/decrypted)
```

null	: 0	1.
des	: 0	1.
3des	: 0	1.
aes	: 0	1.
aes-gcm	: 0	1.
aria	: 0	1.
seed	: 0	1.
chacha20poly1305	: 0	1.

```
Integrity (generated/validated)
```

null	: 0	1.
md5	: 0	1.
sha1	: 0	1.
sha256	: 0	1.
sha384	: 0	1.
sha512	: 0	1.

```
NP6_1:
```

```
Encryption (encrypted/decrypted)
```

null	: 14976	15357
des	: 0	1.
3des	: 0	1.
aes	: 1664	2047
aes-gcm	: 0	1.
aria	: 0	1.
seed	: 0	1.
chacha20poly1305	: 0	1.

```
Integrity (generated/validated)
```

null	: 0	1.
md5	: 1664	2047
sha1	: 14976	15357
sha256	: 0	1.
sha384	: 0	1.
sha512	: 0	1.

```
NPU Host Offloading:
```

```
Encryption (encrypted/decrypted)
```

null	: 3	1.
des	: 0	1.
3des	: 0	1.
aes	: 3	1.
aes-gcm	: 0	1.
aria	: 0	1.
seed	: 0	1.
chacha20poly1305	: 0	1.

```
Integrity (generated/validated)
```

null	: 0	1.
md5	: 3	1.
sha1	: 3	1.
sha256	: 0	1.

```

 sha384 : 0 1.
 sha512 : 0 1.

CP8:
 Encryption (encrypted/decrypted)
 null : 1 1.
 des : 0 1.
 3des : 0 1.
 aes : 1 1.
 aes-gcm : 0 1.
 aria : 0 1.
 seed : 0 1.
 chacha20poly1305 : 0 1.
 Integrity (generated/validated)
 null : 0 1.
 md5 : 1 1.
 sha1 : 1 1.
 sha256 : 0 1.
 sha384 : 0 1.
 sha512 : 0 1.

SOFTWARE:
 Encryption (encrypted/decrypted)
 null : 0 1.
 des : 0 1.
 3des : 0 1.
 aes : 0 1.
 aes-gcm : 29882 29882
 aria : 21688 21688
 seed : 153774 153774
 chacha20poly1305 : 29521 29521
 Integrity (generated/validated)
 null : 59403 59403
 md5 : 0 1.
 sha1 : 175462 175462
 sha256 : 0 1.
 sha384 : 0 1.
 sha512 : 0 1.

```

5. If traffic cannot be offloaded by the NPU, the CP will try to encrypt/decrypt the IPsec packets.

## IPsec traffic processed by CP

1. Check the NPU flag and CP counter.

```

diagnose vpn tunnel list
list all ipsec tunnel in vd 0

name=test ver=2 serial=1 173.1.1.1:0->11.101.1.1:0
bound_if=42 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refcnt=13 ilast=0 olast=0 ad=/0
stat: rxp=8418 txp=8418 rxb=1251248 txb=685896
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=test proto=0 sa=1 ref=3 serial=7
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0

```

```

SA: ref=3 options=10226 type=00 soft=0 mtu=1438 expire=42037/0B replaywin=2048
 seqno=20e3 esn=0 replaywin_lastseq=000020e3 itn=0
life: type=01 bytes=0/0 timeout=42928/43200
dec: spi=e313ac48 esp=aes key=16 393770842f926266530db6e43e21c4f8
 ah=md5 key=16 b2e4e025e8910e95c1745e7855479cca
enc: spi=706ffe05 esp=aes key=16 7ef749610335f9f50e252023926de29e
 ah=md5 key=16 0b81e4d835919ab2b8ba8edbd01aec9d
dec:pkts/bytes=8418/685896, enc:pkts/bytes=8418/1251248
npu_flag=00 npu_rgwy=11.101.1.1 npu_lgwy=173.1.1.1 npu_selid=6 dec_npuid=0 enc_npuid=0

```

FGT-D # diagnose vpn ipsec status

All ipsec crypto devices in use:

NP6\_0:

```

Encryption (encrypted/decrypted)
null : 0 1.
des : 0 1.
3des : 0 1.
aes : 0 1.
aes-gcm : 0 1.
aria : 0 1.
seed : 0 1.
chacha20poly1305 : 0 1.
Integrity (generated/validated)
null : 0 1.
md5 : 0 1.
sha1 : 0 1.
sha256 : 0 1.
sha384 : 0 1.
sha512 : 0 1.

```

NP6\_1:

```

Encryption (encrypted/decrypted)
null : 14976 15357
des : 0 1.
3des : 0 1.
aes : 1664 2047
aes-gcm : 0 1.
aria : 0 1.
seed : 0 1.
chacha20poly1305 : 0 1.
Integrity (generated/validated)
null : 0 1.
md5 : 1664 2047
sha1 : 14976 15357
sha256 : 0 1.
sha384 : 0 1.
sha512 : 0 1.

```

NPU Host Offloading:

```

Encryption (encrypted/decrypted)
null : 3 1.
des : 0 1.
3des : 0 1.
aes : 3 1.
aes-gcm : 0 1.
aria : 0 1.

```

```

 seed : 0 1.
 chacha20poly1305 : 0 1.
 Integrity (generated/validated)
 null : 0 1.
 md5 : 3 1.
 sha1 : 3 1.
 sha256 : 0 1.
 sha384 : 0 1.
 sha512 : 0 1.

CP8:
 Encryption (encrypted/decrypted)
 null : 1 1.
 des : 0 1.
 3des : 0 1.
 aes : 8499 8499
 aes-gcm : 0 1.
 aria : 0 1.
 seed : 0 1.
 chacha20poly1305 : 0 1.
 Integrity (generated/validated)
 null : 0 1.
 md5 : 8499 8499
 sha1 : 1 1.
 sha256 : 0 1.
 sha384 : 0 1.
 sha512 : 0 1.

SOFTWARE:
 Encryption (encrypted/decrypted)
 null : 0 1.
 des : 0 1.
 3des : 0 1.
 aes : 0 1.
 aes-gcm : 29882 29882
 aria : 21688 21688
 seed : 153774 153774
 chacha20poly1305 : 29521 29521
 Integrity (generated/validated)
 null : 59403 59403
 md5 : 0 1.
 sha1 : 175462 175462
 sha256 : 0 1.
 sha384 : 0 1.
 sha512 : 0 1.

```

2. Two options are used to control if the CP processes packets. If disabled, packets are processed by the CPU.

```

config system global
 set ipsec-asic-offload disable
 set ipsec-hmac-offload disable
end

```



## IPsec traffic processed by CPU

IPsec traffic might be processed by the CPU for the following reasons:

- Some low end models do not have NPUs.
- NPU offloading and CP IPsec traffic processing manually disabled.
- Some types of proposals - SEED, ARIA, chacha20poly1305 - are not supported by the NPU or CP.
- NPU flag set to 00 and software encrypt/decrypt counter ticked.

```
diagnose vpn tunnel list
list all ipsec tunnel in vd 0

name=test ver=2 serial=1 173.1.1.1:0->11.101.1.1:0
bound_if=42 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=0 refcnt=14 ilast=0 olast=0 ad=/0
stat: rxp=12162 txp=12162 rxb=1691412 txb=1008216
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=test proto=0 sa=1 ref=4 serial=8
 src: 0:0.0.0.0/0.0.0.0:0
 dst: 0:0.0.0.0/0.0.0.0:0
 SA: ref=3 options=10602 type=00 soft=0 mtu=1453 expire=42903/0B replaywin=2048
 seqno=2d70 esn=0 replaywin_lastseq=00002d70 itn=0
 life: type=01 bytes=0/0 timeout=42931/43200
 dec: spi=e313ac4d esp=chacha20poly1305 key=36
812d1178784c1130d1586606e44e1b9ab157e31a09edbed583be1e9cc82e8c9f2655a2cf
 ah=null key=0
 enc: spi=706ffe0a esp=chacha20poly1305 key=36
f2727e001e2243549b140f1614ae3df82243adb070e60c33911f461b389b05a7a642e11a
 ah=null key=0
 dec:pkts/bytes=11631/976356, enc:pkts/bytes=11631/1627692
 npu_flag=00 npu_rgw=11.101.1.1 npu_lgwy=173.1.1.1 npu_selid=7 dec_npuid=0 enc_npuid=0

FGT_900D # diagnose vpn ipsec status
All ipsec crypto devices in use:
NP6_0:
 Encryption (encrypted/decrypted)
 null : 0 1.
 des : 0 1.
 3des : 0 1.
 aes : 0 1.
 aes-gcm : 0 1.
 aria : 0 1.
 seed : 0 1.
 chacha20poly1305 : 0 1.
 Integrity (generated/validated)
 null : 0 1.
 md5 : 0 1.
 sha1 : 0 1.
 sha256 : 0 1.
 sha384 : 0 1.
 sha512 : 0 1.

NP6_1:
 Encryption (encrypted/decrypted)
 null : 14976 15357
```

des	: 0	1.
3des	: 0	1.
aes	: 1664	2047
aes-gcm	: 0	1.
aria	: 0	1.
seed	: 0	1.
chacha20poly1305	: 0	1.
Integrity (generated/validated)		
null	: 0	1.
md5	: 1664	2047
sha1	: 14976	15357
sha256	: 0	1.
sha384	: 0	1.
sha512	: 0	1.

## NPU Host Offloading:

Encryption (encrypted/decrypted)		
null	: 3	1.
des	: 0	1.
3des	: 0	1.
aes	: 3	1.
aes-gcm	: 0	1.
aria	: 0	1.
seed	: 0	1.
chacha20poly1305	: 0	1.
Integrity (generated/validated)		
null	: 0	1.
md5	: 3	1.
sha1	: 3	1.
sha256	: 0	1.
sha384	: 0	1.
sha512	: 0	1.

## CP8:

Encryption (encrypted/decrypted)		
null	: 1	1.
des	: 0	1.
3des	: 0	1.
aes	: 8865	8865
aes-gcm	: 0	1.
aria	: 0	1.
seed	: 0	1.
chacha20poly1305	: 0	1.
Integrity (generated/validated)		
null	: 0	1.
md5	: 8865	8865
sha1	: 1	1.
sha256	: 0	1.
sha384	: 0	1.
sha512	: 0	1.

## SOFTWARE:

Encryption (encrypted/decrypted)		
null	: 0	1.
des	: 0	1.
3des	: 0	1.

aes	: 531	531
aes-gcm	: 29882	29882
aria	: 21688	21688
seed	: 153774	153774
chacha20poly1305	: 41156	41156
Integrity (generated/validated)		
null	: 71038	71038
md5	: 531	531
sha1	: 175462	175462
sha256	: 0	1.
sha384	: 0	1.
sha512	: 0	1.

## Disable automatic ASIC offloading

When `auto-asic-offload` is set to `disable` in the firewall policy, traffic is not offloaded and the NPU hosting counter is ticked.

```
diagnose vpn ipsec status
All ipsec crypto devices in use:
NP6_0:
 Encryption (encrypted/decrypted)
 null : 0 1.
 des : 0 1.
 3des : 0 1.
 aes : 0 1.
 aes-gcm : 0 1.
 aria : 0 1.
 seed : 0 1.
 chacha20poly1305 : 0 1.
 Integrity (generated/validated)
 null : 0 1.
 md5 : 0 1.
 sha1 : 0 1.
 sha256 : 0 1.
 sha384 : 0 1.
 sha512 : 0 1.

NP6_1:
 Encryption (encrypted/decrypted)
 null : 14976 15357
 des : 0 1.
 3des : 0 1.
 aes : 110080 2175
 aes-gcm : 0 1.
 aria : 0 1.
 seed : 0 1.
 chacha20poly1305 : 0 1.
 Integrity (generated/validated)
 null : 0 1.
 md5 : 110080 2175
 sha1 : 14976 15357
 sha256 : 0 1.
 sha384 : 0 1.
 sha512 : 0 1.
```

## NPU Host Offloading:

## Encryption (encrypted/decrypted)

null	: 3	1.
des	: 0	1.
3des	: 0	1.
aes	: 111090	1.
aes-gcm	: 0	1.
aria	: 0	1.
seed	: 0	1.
chacha20poly1305	: 0	1.

## Integrity (generated/validated)

null	: 0	1.
md5	: 111090	1.
sha1	: 3	1.
sha256	: 0	1.
sha384	: 0	1.
sha512	: 0	1.

## CP8:

## Encryption (encrypted/decrypted)

null	: 1	1.
des	: 0	1.
3des	: 0	1.
aes	: 8865	8865
aes-gcm	: 0	1.
aria	: 0	1.
seed	: 0	1.
chacha20poly1305	: 0	1.

## Integrity (generated/validated)

null	: 0	1.
md5	: 8865	8865
sha1	: 1	1.
sha256	: 0	1.
sha384	: 0	1.
sha512	: 0	1.

## SOFTWARE:

## Encryption (encrypted/decrypted)

null	: 0	1.
des	: 0	1.
3des	: 0	1.
aes	: 539	539
aes-gcm	: 29882	29882
aria	: 21688	21688
seed	: 153774	153774
chacha20poly1305	: 41259	41259

## Integrity (generated/validated)

null	: 71141	71141
md5	: 539	539
sha1	: 175462	175462
sha256	: 0	1.
sha384	: 0	1.
sha512	: 0	1.

## Encryption algorithms

This topic provides a brief introduction to IPsec phase 1 and phase 2 encryption algorithms and includes the following sections:

- [IKEv1 phase 1 encryption algorithm](#)
- [IKEv1 phase 2 encryption algorithm](#)
- [IKEv2 phase 1 encryption algorithm](#)
- [IKEv2 phase 2 encryption algorithm](#)
- [HMAC settings](#)

### IKEv1 phase 1 encryption algorithm

The default encryption algorithm is:

```
aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
```

DES is a symmetric-key algorithm, which means the same key is used for encrypting and decrypting data. FortiOS supports:

- des-md5
- des-sha1
- des-sha256
- des-sha384
- des-sha512

3DES applies the DES algorithm three times to each data. FortiOS supports:

- 3des-md5
- 3des-sha1
- 3des-sha256
- 3des-sha384
- 3des-sha512

AES is a symmetric-key algorithm with different key lengths (128, 192, and 256 bits). FortiOS supports:

- aes128-md5
- aes128-sha1
- aes128-sha256
- aes128-sha384
- aes128-sha512
- aes192-md5
- aes192-sha1
- aes192-sha256
- aes192-sha384
- aes192-sha512
- aes256-md5
- aes256-sha1
- aes256-sha256
- aes256-sha384
- aes256-sha512

The ARIA algorithm is based on AES with different key lengths (128, 192, and 256 bits). FortiOS supports:

- aria128-md5
- aria128-sha1
- aria128-sha256
- aria128-sha384
- aria128-sha512
- aria192-md5
- aria192-sha1
- aria192-sha256
- aria192-sha384
- aria192-sha512
- aria256-md5
- aria256-sha1
- aria256-sha256
- aria256-sha384
- aria256-sha512

SEED is a symmetric-key algorithm. FortiOS supports:

- seed128-md5
- seed128-sha1
- seed128-sha256
- seed128-sha384
- seed128-sha512

Suite-B is a set of AES encryption with ICV in GCM mode. FortiOS supports Suite-B on new kernel platforms only (kernel version 3 and above). IPsec traffic can be offloaded on NP6XLite and NP7 platforms. They cannot be offloaded on other NP6 processors and below. CP9 supports Suite-B offloading, otherwise packets are encrypted and decrypted by software. FortiOS supports:

- suite-b-gcm-128
- suite-b-gcm-256

See [Network processors \(NP6, NP6XLite, NP6Lite, and NP4\)](#) and [CP9, CP9XLite, and CP9Lite](#) capabilities in the Hardware Acceleration guide for more information.

## IKEv1 phase 2 encryption algorithm

The default encryption algorithm is:

```
aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
```

With null encryption, IPsec traffic can offload NPU/CP. FortiOS supports:

- null-md5
- null-sha1
- null-sha256
- null-sha384
- null-sha512

With the DES encryption algorithm, IPsec traffic can offload NPU/CP. FortiOS supports:

- des-null
- des-md5
- des-sha1
- des-sha256
- des-sha384
- des-sha512

With the 3DES encryption algorithm, IPsec traffic can offload NPU/CP. FortiOS supports:

- 3des-null
- 3des-md5
- 3des-sha1
- 3des-sha256
- 3des-sha384
- 3des-sha512

With the AES encryption algorithm, IPsec traffic can offload NPU/CP. FortiOS supports:

- aes128-null
- aes128-md5
- aes128-sha1
- aes128-sha256
- aes128-sha384
- aes128-sha512
- aes192-null
- aes192-md5
- aes192-sha1
- aes192-sha256
- aes192-sha384
- aes192-sha512
- aes256-null
- aes256-md5
- aes256-sha1
- aes256-sha256
- aes256-sha384
- aes256-sha512

With the AESGCM encryption algorithm, IPsec traffic **cannot** offload NPU/CP. FortiOS supports:

- aes128gcm
- aes256gcm

With the chacha20poly1305 encryption algorithm, IPsec traffic **cannot** offload NPU/CP. FortiOS supports:

- chacha20poly1305

With the ARIA encryption algorithm, IPsec traffic **cannot** offload NPU/CP. FortiOS supports:

- aria128-null
- aria128-md5
- aria128-sha1

- aria128-sha256
- aria128-sha384
- aria128-sha512
- aria192-null
- aria192-md5
- aria192-sha1
- aria192-sha256
- aria192-sha384
- aria192-sha512
- aria256-null
- aria256-md5
- aria256-sha1
- aria256-sha256
- aria256-sha384
- aria256-sha512

With the SEED encryption algorithm, IPsec traffic **cannot** offload NPU/CP. FortiOS supports:

- seed-null
- seed-md5
- seed-sha1
- seed-sha256
- seed-sha384
- seed-sha512

## IKEv2 phase 1 encryption algorithm

The default encryption algorithm is:

aes128-sha256 aes256-sha256 aes128gcm-prfsha256 aes256gcm-prfsha384 chacha20poly1305-prfsha256

DES is a symmetric-key algorithm, which means the same key is used for encrypting and decrypting data. FortiOS supports:

- des-md5
- des-sha1
- des-sha256
- des-sha384
- des-sha512

3DES applies the DES algorithm three times to each data. FortiOS supports:

- 3des-md5
- 3des-sha1
- 3des-sha256
- 3des-sha384
- 3des-sha512



AES is a symmetric-key algorithm with different key lengths (128, 192, and 256 bits). FortiOS supports:

- aes128-md5
- aes128-sha1
- aes128-sha256
- aes128-sha384
- aes128-sha512
- aes128gcm-prfsha1
- aes128gcm-prfsha256
- aes128gcm-prfsha384
- aes128gcm-prfsha512
- aes192-md5
- aes192-sha1
- aes192-sha256
- aes192-sha384
- aes192-sha512
- aes256-md5
- aes256-sha1
- aes256-sha256
- aes256-sha384
- aes256-sha512
- aes256gcm-prfsha1
- aes256gcm-prfsha256
- aes256gcm-prfsha384
- aes256gcm-prfsha512

The ARIA algorithm is based on AES with different key lengths (128, 192, and 256 bits). FortiOS supports:

- aria128-md5
- aria128-sha1
- aria128-sha256
- aria128-sha384
- aria128-sha512
- aria192-md5
- aria192-sha1
- aria192-sha256
- aria192-sha384
- aria192-sha512
- aria256-md5
- aria256-sha1
- aria256-sha256
- aria256-sha384
- aria256-sha512

With the chacha20poly1305 encryption algorithm, FortiOS supports:

- chacha20poly1305-prfsha1
- chacha20poly1305-prfsha256

- chacha20poly1305-prfsha384
- chacha20poly1305-prfsha512

SEED is a symmetric-key algorithm. FortiOS supports:

- seed128-md5
- seed128-sha1
- seed128-sha256
- seed128-sha384
- seed128-sha512

Suite-B is a set of AES encryption with ICV in GCM mode. FortiOS supports Suite-B on new kernel platforms only (kernel version 3 and above). IPsec traffic can be offloaded on NP6X Lite and NP7 platforms. They cannot be offloaded on other NP6 processors and below. CP9 supports Suite-B offloading, otherwise packets are encrypted and decrypted by software. FortiOS supports:

- suite-b-gcm-128
- suite-b-gcm-256

See [Network processors \(NP6, NP6X Lite, NP6 Lite, and NP4\)](#) and [CP9, CP9X Lite, and CP9 Lite](#) capabilities in the Hardware Acceleration guide for more information.

## IKEv2 phase 2 encryption algorithm

The default encryption algorithm is:

```
aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm aes256gcm chacha20poly1305
```

With null encryption, IPsec traffic can offload NPU/CP. FortiOS supports:

- null-md5
- null-sha1
- null-sha256
- null-sha384
- null-sha512

With the DES encryption algorithm, IPsec traffic can offload NPU/CP. FortiOS supports:

- des-null
- des-md5
- des-sha1
- des-sha256
- des-sha384
- des-sha512

With the 3DES encryption algorithm, IPsec traffic can offload NPU/CP. FortiOS supports:

- 3des-null
- 3des-md5
- 3des-sha1
- 3des-sha256
- 3des-sha384
- 3des-sha512

With the AES encryption algorithm, IPsec traffic can offload NPU/CP. FortiOS supports:

- aes128-null
- aes128-md5
- aes128-sha1
- aes128-sha256
- aes128-sha384
- aes128-sha512
- aes192-null
- aes192-md5
- aes192-sha1
- aes192-sha256
- aes192-sha384
- aes192-sha512
- aes256-null
- aes256-md5
- aes256-sha1
- aes256-sha256
- aes256-sha384
- aes256-sha512

With the AESGCM encryption algorithm, IPsec traffic **cannot** offload NPU. CP9 supports AESGCM offloading. FortiOS supports:

- aes128gcm
- aes256gcm

With the chacha20poly1305 encryption algorithm, IPsec traffic **cannot** offload NPU/CP. FortiOS supports:

- chacha20poly1305

With the ARIA encryption algorithm, IPsec traffic **cannot** offload NPU/CP. FortiOS supports:

- aria128-null
- aria128-md5
- aria128-sha1
- aria128-sha256
- aria128-sha384
- aria128-sha512
- aria192-null
- aria192-md5
- aria192-sha1
- aria192-sha256
- aria192-sha384
- aria192-sha512
- aria256-null
- aria256-md5
- aria256-sha1
- aria256-sha256

- aria256-sha384
- aria256-sha512

With the SEED encryption algorithm, IPsec traffic **cannot** offload NPU/CP. FortiOS supports:

- seed-null
- seed-md5
- seed-sha1
- seed-sha256
- seed-sha384
- seed-sha512

## HMAC settings

The FortiGate uses the HMAC based on the authentication proposal that is chosen in phase 1 or phase 2 of the IPsec configuration. Each proposal consists of the encryption-hash pair (such as 3des-sha256). The FortiGate matches the most secure proposal to negotiate with the peer.

### To view the chosen proposal and the HMAC hash used:

```
diagnose vpn ike gateway list

vd: root/0
name: MPLS
version: 1
interface: port1 3
addr: 192.168.2.5:500 -> 10.10.10.1:500
virtual-interface-addr: 172.31.0.2 -> 172.31.0.1
created: 1015820s ago
IKE SA: created 1/13 established 1/13 time 10/1626/21010 ms
IPsec SA: created 1/24 established 1/24 time 0/11/30 ms

id/spi: 124 43b087dae99f7733/6a8473e58cd8990a
direction: responder
status: established 68693-68693s ago = 10ms
proposal: 3des-sha256
key: e0fa6ab8dc509b33-aa2cc549999b1823-c3cb9c337432646e
lifetime/rekey: 86400/17436
DPD sent/recv: 000001e1/00000000
```

## Fragmenting IP packets before IPsec encapsulation

The `ip-fragmentation` command controls packet fragmentation before IPsec encapsulation, which can benefit packet loss in some environments.

The following options are available for the `ip-fragmentation` variable.

Option	Description
pre-encapsulation	Fragment before IPsec encapsulation.
post-encapsulation (default value)	Fragment after IPsec encapsulation (RFC compliant).

### To configure packet fragmentation using the CLI:

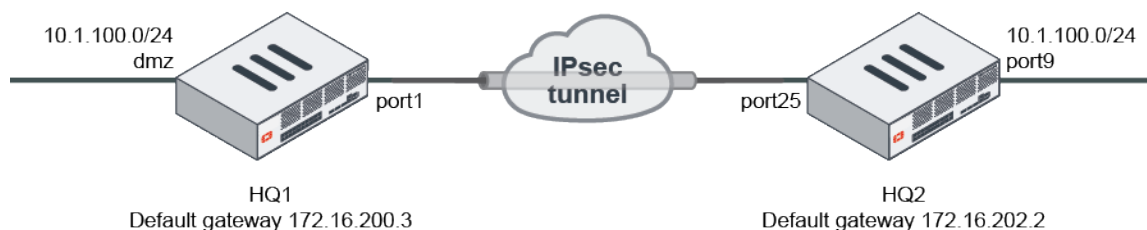
```
config vpn ipsec phase1-interface
edit "demo"
 set interface "port1"
 set authmethod signature
 set peertype any
 set net-device enable
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set ip-fragmentation pre-encapsulation
 set remote-gw 172.16.200.4
 set certificate "Fortinet_Factory"
next
end
```

## VXLAN over IPsec tunnel

This is an example of VXLAN over IPsec tunnel. VXLAN encapsulation is used in the `phase1-interface` setting and virtual-switch is used to bridge the internal with VXLAN over IPsec tunnel.

For more information, see .

### Sample topology



### Sample configuration

#### To configure VXLAN over an IPsec tunnel:

##### 1. Configure the WAN interface and default route:

###### a. HQ1:

```
config system interface
edit "port1"
 set ip 172.16.200.1 255.255.255.0
next
end
config router static
edit 1
 set gateway 172.16.200.3
 set device "port1"
next
end
```

**b. HQ2:**

```

config system interface
 edit "port25"
 set ip 172.16.202.1 255.255.255.0
 next
end
config router static
 edit 1
 set gateway 172.16.202.2
 set device "port25"
 next
end

```

**2. Configure IPsec phase1-interface:****a. HQ1:**

```

config vpn ipsec phase1-interface
 edit "to_HQ2"
 set interface "port1"
 set peertype any
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set encapsulation VXLAN
 set encapsulation-address ipv4
 set encap-local-gw4 172.16.200.1
 set encap-remote-gw4 172.16.202.1
 set remote-gw 172.16.202.1
 set psksecret sample
 next
end
config vpn ipsec phase2-interface
 edit "to_HQ2"
 set phase1name "to_HQ2"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305
 next
end

```

**b. HQ2:**

```

config vpn ipsec phase1-interface
 edit "to_HQ1"
 set interface "port25"
 set peertype any
 set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
 set encapsulation VXLAN
 set encapsulation-address ipv4
 set encap-local-gw4 172.16.202.1
 set encap-remote-gw4 172.16.200.1
 set remote-gw 172.16.200.1
 set psksecret sample
 next
end
config vpn ipsec phase2-interface
 edit "to_HQ1"
 set phase1name "to_HQ1"
 set proposal aes128-sha1 aes256-sha1 aes128-sha256 aes256-sha256 aes128gcm
 aes256gcm chacha20poly1305

```

```
 next
end
```

### 3. Configure the virtual switch.

#### a. HQ1

```
config system switch-interface
 edit "VXLAN-HQ2"
 set member "dmz" "to_HQ2"
 set intra-switch-policy explicit
 next
end
```

#### b. HQ2

```
config system switch-interface
 edit "VXLAN-HQ1"
 set member "port9" "to_HQ1"
 set intra-switch-policy explicit
 next
end
```

### 4. Configure the firewall policy:

#### a. HQ1:

```
config firewall policy
 edit 1
 set srcintf "dmz"
 set dstintf "to_HQ2"
 set srcaddr "10.1.100.0"
 set dstaddr "10.1.100.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set srcintf "to_HQ2"
 set dstintf "dmz"
 set srcaddr "10.1.100.0"
 set dstaddr "10.1.100.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end
```

#### b. HQ2:

```
config firewall policy
 edit 1
 set srcintf "port9"
 set dstintf "to_HQ1"
 set srcaddr "10.1.100.0"
 set dstaddr "10.1.100.0"
 set action accept
 set schedule "always"
 set service "ALL"
 next
```

```

edit 2
 set srcintf "to_HQ1"
 set dstintf "port9"
 set srcaddr "10.1.100.0"
 set dstaddr "10.1.100.0"
 set action accept
 set schedule "always"
 set service "ALL"
next
end

```

**5. Optionally, view the VPN tunnel list on HQ1 with the diagnose vpn tunnel list command:**

```

list all ipsec tunnel in vd 0

name=to_HQ2 ver=1 serial=2 172.16.200.1:0->172.16.202.1:0
bound_if=5 lgwy=static/1 tun=intf/0 mode=auto/1 encap=VXLAN/2 options[0002]=
encap-addr: 172.16.200.1->172.16.202.1
proxyid_num=1 child_num=0 refcnt=11 ilast=8 olast=0 ad=/0
stat: rxp=13 txp=3693 rxb=5512 txb=224900
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=45
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=to_HQ2 proto=0 sa=1 ref=2 serial=1
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=3 options=10226 type=00 soft=0 mtu=1390 expire=41944/0B replaywin=2048
seqno=e6e esn=0 replaywin_lastseq=0000000e itn=0
life: type=01 bytes=0/0 timeout=42901/43200
dec: spi=635e9bb1 esp=aes key=16 c8a374905ef9156e66504195f46a650c
ah=sha1 key=20 a09265de7d3b0620b45441fb5af44dab125f2afe
enc: spi=a4d0cd1e esp=aes key=16 e9d0f3f0bb7e15a833f80c42615a3b91
ah=sha1 key=20 609a315c385471b8909b771c76e4fa7214996e50
dec:pkts/bytes=13/4640, enc:pkts/bytes=3693/623240

```

**6. Optionally, view the bridge control interface on HQ1 with the diagnose netlink brctl name host VXLAN-HQ1 command:**

```

show bridge control interface VXLAN-HQ1 host.
fdb: size=2048, used=17, num=17, depth=1
Bridge VXLAN-a host table

```

port	no	device	devname	mac	addr	ttl	attributes
1	1.	dmz	00:0c:29:4e:33:c9	1.	Hit(1)		
1	1.	dmz	00:0c:29:a8:c3:ea	105	Hit(105)		
1	1.	dmz	90:6c:ac:53:76:29	18	Hit(18)		
1	1.	dmz	08:5b:0e:dd:69:cb	1.	Local Static		
1	1.	dmz	90:6c:ac:84:3e:5d	1.	Hit(5)		
1	1.	dmz	00:0b:fd:eb:21:d6	1.	Hit(0)		
2	38	to_HQ2	56:45:c3:3f:57:b4	1.	Local Static		
1	1.	dmz	00:0c:29:d2:66:40	78	Hit(78)		
2	38	to_HQ2	90:6c:ac:5b:a6:eb	124	Hit(124)		
1	1.	dmz	00:0c:29:a6:bc:e6	19	Hit(19)		
1	1.	dmz	00:0c:29:f0:a2:e7	1.	Hit(0)		
1	1.	dmz	00:0c:29:d6:c4:66	164	Hit(164)		
1	1.	dmz	00:0c:29:e7:68:19	1.	Hit(0)		
1	1.	dmz	00:0c:29:bf:79:30	19	Hit(19)		
1	1.	dmz	00:0c:29:e0:64:7d	1.	Hit(0)		



1	1.	dmz	36:ea:c7:30:c0:f1	25	Hit (25)
1	1.	dmz	36:ea:c7:30:cc:71	1.	Hit (0)

## VPN IPsec troubleshooting

See the following IPsec troubleshooting examples:

- [Understanding VPN related logs](#)
- [IPsec related diagnose command on page 1365](#)

### Understanding VPN related logs

This section provides some IPsec log samples.

#### IPsec phase1 negotiating

```
logid="0101037127" type="event" subtype="vpn" level="notice" vd="root" eventtime=1544132571
logdesc="Progress IPsec phase 1" msg="progress IPsec phase 1" action="negotiate"
remip=11.101.1.1

locip=173.1.1.1 remport=500 locport=500 outintf="port13"
cookies="e41eeecb2c92b337/0000000000000000" user="N/A" group="N/A" xauthuser="N/A"
xauthgroup="N/A" assignip=N/A vpntunnel="to_HQ" status="success" init="local"
mode="aggressive" dir="outbound" stage=1 role="initiator" result="OK"
```

#### IPsec phase1 negotiated

```
logid="0101037127" type="event" subtype="vpn" level="notice" vd="root" eventtime=1544132571
logdesc="Progress IPsec phase 1" msg="progress IPsec phase 1" action="negotiate"
remip=11.101.1.1

locip=173.1.1.1 remport=500 locport=500 outintf="port13"
cookies="e41eeecb2c92b337/1230131a28eb4e73" user="N/A" group="N/A" xauthuser="N/A"
xauthgroup="N/A" assignip=N/A vpntunnel="to_HQ" status="success" init="local"

mode="aggressive" dir="outbound" stage=2 role="initiator" result="DONE"
```

#### IPsec phase1 tunnel up

```
logid="0101037138" type="event" subtype="vpn" level="notice" vd="root" eventtime=1544132604
logdesc="IPsec connection status changed" msg="IPsec connection status change"
action="tunnel-up" remip=11.101.1.1 locip=173.1.1.1 remport=500 locport=500 outintf="port13"
cookies="5b1c59fab2029e43/bf517e686d3943d2" user="N/A" group="N/A" xauthuser="N/A"
xauthgroup="N/A" assignip=11.11.11.1 vpntunnel="to_HQ" tunnelip=N/A tunnelid=1530910918
tunneltype="ipsec" duration=0 sentbyte=0 rcvdbyte=0 nextstat=0
```

#### IPsec phase2 negotiate

```
logid="0101037129" type="event" subtype="vpn" level="notice" vd="root" eventtime=1544132604
logdesc="Progress IPsec phase 2" msg="progress IPsec phase 2" action="negotiate"
remip=11.101.1.1
```

```
locip=173.1.1.1 remport=500 locport=500 outintf="port13"
cookies="5b1c59fab2029e43/bf517e686d3943d2" user="N/A" group="N/A" xauthuser="N/A"
xauthgroup="N/A" assignip=11.11.11.1 vpntunnel="to_HQ" status="success" init="local"

mode="quick" dir="outbound" stage=1 role="initiator" result="OK"
```

### IPsec phase2 tunnel up

```
logid="0101037139" type="event" subtype="vpn" level="notice" vd="root" eventtime=1544132604
logdesc="IPsec phase 2 status changed" msg="IPsec phase 2 status change" action="phase2-up"

 remip=11.101.1.1 locip=173.1.1.1 remport=500 locport=500 outintf="port13"
 cookies="5b1c59fab2029e43/bf517e686d3943d2" user="N/A" group="N/A" xauthuser="N/A"
 xauthgroup="N/A" assignip=11.11.11.1 vpntunnel="to_HQ"

phase2_name="to_HQ"
```

### IPsec phase2 sa install

```
logid="0101037133" type="event" subtype="vpn" level="notice" vd="root" eventtime=1544132604
logdesc="IPsec SA installed" msg="install IPsec SA" action="install_sa" remip=11.101.1.1
locip=173.1.1.1

 remport=500 locport=500 outintf="port13" cookies="5b1c59fab2029e43/bf517e686d3943d2"
 user="N/A" group="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=11.11.11.1
 vpntunnel="to_HQ" role="initiator" in_spi="ca646448" out_spi="747c10c6"
```

### IPsec tunnel statistics

```
logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" eventtime=1544131118
logdesc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunnel-stats"
remip=10.1.100.15 locip=172.16.200.4 remport=500 locport=500 outintf="mgmt1"
cookies="3539884dbd8f3567/c32e4c1beca91b36"

 user="N/A" group="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A
 vpntunnel="L2tpoIPsec_0" tunnelip=10.1.100.15 tunnelid=1530910802 tunneltype="ipsec"
 duration=6231 sentbyte=57343 rcvdbyte=142640 nextstat=60
```

### IPsec phase2 tunnel down

```
logid="0101037138" type="event" subtype="vpn" level="notice" vd="root" eventtime=1544132571
logdesc="IPsec connection status changed" msg="IPsec connection status change"
action="tunnel-down" remip=11.101.1.1 locip=173.1.1.1 remport=500 locport=500
outintf="port13" cookies="30820aa390687e39/886e72bf5461fb8d" user="N/A" group="N/A"
xauthuser="N/A" xauthgroup="N/A" assignip=11.11.11.1 vpntunnel="to_HQ" tunnelip=N/A
tunnelid=1530910786 tunneltype="ipsec" duration=6425 sentbyte=504 rcvdbyte=152 nextstat=0
```

### IPsec phase1 sa deleted

```
logid="0101037134" type="event" subtype="vpn" level="notice" vd="root" eventtime=1544132571
logdesc="IPsec phase 1 SA deleted" msg="delete IPsec phase 1 SA" action="delete_phase1_sa"
remip=11.101.1.1 locip=173.1.1.1 remport=500 locport=500 outintf="port13"
cookies="30820aa390687e39/886e72bf5461fb8d" user="N/A" group="N/A" xauthuser="N/A"
xauthgroup="N/A" assignip=11.11.11.1 vpntunnel="to_HQ"
```

## IPsec related diagnose command

This section provides IPsec related diagnose commands.

- **Daemon IKE summary information list:** `diagnose vpn ike status`
- **IPsec phase1 interface status:** `diagnose vpn ike gateway list`

```
connection: 2/50
IKE SA: created 2/51 established 2/9 times 0/13/40 ms
IPsec SA: created 1/13 established 1/7 times 0/8/30 ms
```

```
vd: root/0
name: tofgtc
version: 1
interface: port13 42
addr: 173.1.1.1:500 -> 172.16.200.3:500
created: 4313s ago
IKE SA: created 1/1 established 1/1 time 10/10/10 ms
IPsec SA: created 0/0
```

```
id/spi: 92 5639f7f8a5dc54c0/809a6c9bbd266a4b
direction: initiator
status: established 4313-4313s ago = 10ms
proposal: aes128-sha256
key: 74aa3d63d88e10ea-8alc73b296b06578
lifetime/rekey: 86400/81786
DPD sent/recv: 00000000/00000000
```

```
vd: root/0
name: to_HQ
version: 1
interface: port13 42
addr: 173.1.1.1:500 -> 11.101.1.1:500
created: 1013s ago
assigned IPv4 address: 11.11.11.1/255.255.255.252
IKE SA: created 1/1 established 1/1 time 0/0/0 ms
IPsec SA: created 1/1 established 1/1 time 0/0/0 ms
```

```
id/spi: 95 255791bd30c749f4/c2505db65210258b
direction: initiator
status: established 1013-1013s ago = 0ms
proposal: aes128-sha256
key: bb101b9127ed5844-1582fd614d5a8a33
lifetime/rekey: 86400/85086
DPD sent/recv: 00000000/00000010
```

- **IPsec phase2 tunnel status:** `diagnose vpn tunnel list`

```
list all ipsec tunnel in vd 0

nname=L2tpoIPsec ver=1 serial=6 172.16.200.4:0->0.0.0.0:0
bound_if=4 lgwy=static/1 tun=intf/0 mode=dialup/2 encap=none/24 options[0018]=npu
create_dev
proxyid_num=0 child_num=0 refcnt=10 ilast=13544 olast=13544 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-idle on=0 idle=60000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
```

```

run_tally=0

name=to_HQ ver=1 serial=7 173.1.1.1:0->11.101.1.1:0
bound_if=42 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/8 options[0008]=npu
proxyid_num=1 child_num=0 refcnt=13 ilast=10 olast=1112 ad=/0
stat: rxp=1 txp=4 rxb=152 txb=336
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=5
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=to_HQ proto=0 sa=1 ref=2 serial=1
src: 0:0.0.0.0/0.0.0.0:0
dst: 0:0.0.0.0/0.0.0.0:0
SA: ref=6 options=10226 type=00 soft=0 mtu=1438 expire=41773/0B replaywin=2048
 seqno=5 esn=0 replaywin_lastseq=00000002 itn=0
life: type=01 bytes=0/0 timeout=42900/43200
dec: spi=ca64644a esp=aes key=16 6cc873fdef91337a6cf9b6948972c90f
 ah=sha1 key=20 e576dbe3ff92605931e5670ad57763c50c7dc73a
enc: spi=747c10c8 esp=aes key=16 5060ad8d0da6824204e3596c0bd762f4
 ah=sha1 key=20 52965cbd5b6ad95212fc825929d26c0401948abe
dec:pkts/bytes=1/84, enc:pkts/bytes=4/608
npu_flag=03 npu_rgwy=11.101.1.1 npu_lgwy=173.1.1.1 npu_selid=5 dec_npuid=2 enc_npuid=2

```

- **Packets encrypted/decrypted counter:** diagnose vpn ipsec status

All ipsec crypto devices in use:

NP6\_0:

```

Encryption (encrypted/decrypted)
null : 0 1.
des : 0 1.
3des : 0 1.
aes : 0 1.
aes-gcm : 0 1.
aria : 0 1.
seed : 0 1.
chacha20poly1305 : 0 1.
Integrity (generated/validated)
null : 0 1.
md5 : 0 1.
sha1 : 0 1.
sha256 : 0 1.
sha384 : 0 1.
sha512 : 0 1.

```

NP6\_1:

```

Encryption (encrypted/decrypted)
null : 0 1.
des : 0 1.
3des : 0 1.
aes : 337152 46069
aes-gcm : 0 1.
aria : 0 1.
seed : 0 1.
chacha20poly1305 : 0 1.
Integrity (generated/validated)
null : 0 1.
md5 : 0 1.
sha1 : 337152 46069
sha256 : 0 1.

```

```

 sha384 : 0 1.
 sha512 : 0 1.

NPU Host Offloading:
 Encryption (encrypted/decrypted)
 null : 0 1.
 des : 0 1.
 3des : 0 1.
 aes : 38 1.
 aes-gcm : 0 1.
 aria : 0 1.
 seed : 0 1.
 chacha20poly1305 : 0 1.
 Integrity (generated/validated)
 null : 0 1.
 md5 : 0 1.
 sha1 : 38 1.
 sha256 : 0 1.
 sha384 : 0 1.
 sha512 : 0 1.

CP8:
 Encryption (encrypted/decrypted)
 null : 0 1.
 des : 0 1.
 3des : 1337 1582
 aes : 71 11426
 aes-gcm : 0 1.
 aria : 0 1.
 seed : 0 1.
 chacha20poly1305 : 0 1.
 Integrity (generated/validated)
 null : 0 1.
 md5 : 48 28
 sha1 : 1360 12980
 sha256 : 0 1.
 sha384 : 0 1.
 sha512 : 0 1.

SOFTWARE:
 Encryption (encrypted/decrypted)
 null : 0 1.
 des : 0 1.
 3des : 0 1.
 aes : 0 1.
 aes-gcm : 0 1.
 aria : 0 1.
 seed : 0 1.
 chacha20poly1305 : 0 1.
 Integrity (generated/validated)
 null : 0 1.
 md5 : 0 1.
 sha1 : 0 1.
 sha256 : 0 1.
 sha384 : 0 1.
 sha512 : 0 1.

```

- diagnose debug application ike -1
  - diagnose vpn ike log-filter dst-addr4 11.101.1.1
  - diagnose vpn ike log-filter src-addr4 173.1.1.1

```
ike 0:to_HQ:101: initiator: aggressive mode is sending 1st message...
ike 0:to_HQ:101: cookie dff03f1d4820222a/0000000000000000
ike 0:to_HQ:101: sent IKE msg (agg_i1send): 173.1.1.1:500->11.101.1.1:500, len=912,
id=df03f1d4820222a/0000000000000000
ike 0: comes 11.101.1.1:500->173.1.1.1:500,ifindex=42....
ike 0: IKEv1 exchange=Aggressive id=df03f1d4820222a/6c2caf4dcf5bab75 len=624
ike 0:to_HQ:101: initiator: aggressive mode get 1st response...
ike 0:to_HQ:101: VID RFC 3947 4A131C81070358455C5728F20E95452F
ike 0:to_HQ:101: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:to_HQ:101: DPD negotiated
ike 0:to_HQ:101: VID draft-ietf-ipsra-isakmp-xauth-06.txt 09002689DFD6B712
ike 0:to_HQ:101: VID CISCO-UNITY 12F5F28C457168A9702D9FE274CC0204
ike 0:to_HQ:101: peer supports UNITY
ike 0:to_HQ:101: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:to_HQ:101: peer is [[QualityAssurance62/FortiGate]]/FortiOS (v0 b0)
ike 0:to_HQ:101: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:to_HQ:101: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:to_HQ:101: peer identifier IPV4_ADDR 11.101.1.1
ike 0:to_HQ:101: negotiation result
ike 0:to_HQ:101: proposal id = 1:
ike 0:to_HQ:101: protocol id = ISAKMP:
ike 0:to_HQ:101: trans_id = KEY_IKE.
ike 0:to_HQ:101: encapsulation = IKE/none
ike 0:to_HQ:101: type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:to_HQ:101: type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:to_HQ:101: type=AUTH_METHOD, val=PRESHARED_KEY_XAUTH_I.
ike 0:to_HQ:101: type=OAKLEY_GROUP, val=MODP2048.
ike 0:to_HQ:101: ISAKMP SA lifetime=86400
ike 0:to_HQ:101: received NAT-D payload type 20
ike 0:to_HQ:101: received NAT-D payload type 20
ike 0:to_HQ:101: selected NAT-T version: RFC 3947
ike 0:to_HQ:101: NAT not detected
ike 0:to_HQ:101: ISAKMP SA dff03f1d4820222a/6c2caf4dcf5bab75 key
16:D81CAE6B2500435BFF195491E80148F3
ike 0:to_HQ:101: PSK authentication succeeded
ike 0:to_HQ:101: authentication OK
ike 0:to_HQ:101: add INITIAL-CONTACT
ike 0:to_HQ:101: sent IKE msg (agg_i2send): 173.1.1.1:500->11.101.1.1:500, len=172,
id=df03f1d4820222a/6c2caf4dcf5bab75
ike 0:to_HQ:101: established IKE SA dff03f1d4820222a/6c2caf4dcf5bab75
ike 0: comes 11.101.1.1:500->173.1.1.1:500,ifindex=42....
ike 0: IKEv1 exchange=Mode config id=df03f1d4820222a/6c2caf4dcf5bab75:97d88fb4 len=92
ike 0:to_HQ:101: mode-cfg type 16521 request 0:
ike 0:to_HQ:101: mode-cfg type 16522 request 0:
ike 0:to_HQ:101: sent IKE msg (cfg_send): 173.1.1.1:500->11.101.1.1:500, len=108,
id=df03f1d4820222a/6c2caf4dcf5bab75:97d88fb4
ike 0: comes 11.101.1.1:500->173.1.1.1:500,ifindex=42....
ike 0: IKEv1 exchange=Mode config id=df03f1d4820222a/6c2caf4dcf5bab75:3724f295 len=92
ike 0:to_HQ:101: sent IKE msg (cfg_send): 173.1.1.1:500->11.101.1.1:500, len=92,
id=df03f1d4820222a/6c2caf4dcf5bab75:3724f295
ike 0:to_HQ:101: initiating mode-cfg pull from peer
ike 0:to_HQ:101: mode-cfg request APPLICATION_VERSION
```

```

ike 0:to_HQ:101: mode-cfg request INTERNAL_IP4_ADDRESS
ike 0:to_HQ:101: mode-cfg request INTERNAL_IP4_NETMASK
ike 0:to_HQ:101: mode-cfg request UNITY_SPLIT_INCLUDE
ike 0:to_HQ:101: mode-cfg request UNITY_PFS
ike 0:to_HQ:101: sent IKE msg (cfg_send): 173.1.1.1:500->11.101.1.1:500, len=140,
id=df03f1d4820222a/6c2caf4dcf5bab75:3bca961f
ike 0: comes 11.101.1.1:500->173.1.1.1:500,ifindex=42....
ike 0: IKEv1 exchange=Mode config id=df03f1d4820222a/6c2caf4dcf5bab75:3bca961f len=172
ike 0:to_HQ:101: mode-cfg type 1 response 4:0B0B0B01
ike 0:to_HQ:101: mode-cfg received INTERNAL_IP4_ADDRESS 11.11.11.1
ike 0:to_HQ:101: mode-cfg type 2 response 4:FFFFFFFFC
ike 0:to_HQ:101: mode-cfg received INTERNAL_IP4_NETMASK 255.255.255.252
ike 0:to_HQ:101: mode-cfg received UNITY_PFS 1
ike 0:to_HQ:101: mode-cfg type 28676 response
28:0A016400FFFFFFFF000000000000000A016500FFFFFFFF0000000000000000
ike 0:to_HQ:101: mode-cfg received UNITY_SPLIT_INCLUDE 0 10.1.100.0/255.255.255.0:0
local port 0
ike 0:to_HQ:101: mode-cfg received UNITY_SPLIT_INCLUDE 0 10.1.101.0/255.255.255.0:0
local port 0
ike 0:to_HQ:101: mode-cfg received APPLICATION_VERSION 'FortiGate-100D
v6.0.3,build0200,181009 (GA) '
ike 0:to_HQ: mode-cfg add 11.11.11.1/255.255.255.252 to 'to_HQ'/58
ike 0:to_HQ: set oper up
ike 0:to_HQ: schedule auto-negotiate
ike 0:to_HQ:101: no pending Quick-Mode negotiations
ike shrank heap by 159744 bytes
ike 0:to_HQ:to_HQ: IPsec SA connect 42 173.1.1.1->11.101.1.1:0
ike 0:to_HQ:to_HQ: using existing connection

ike 0:to_HQ:to_HQ: config found
ike 0:to_HQ:to_HQ: IPsec SA connect 42 173.1.1.1->11.101.1.1:500 negotiating
ike 0:to_HQ:101: cookie df03f1d4820222a/6c2caf4dcf5bab75:32f4cc01
ike 0:to_HQ:101:to_HQ:259: initiator selectors 0 0:0.0.0.0/0.0.0.0:0-
>0:0.0.0.0/0.0.0.0:0:0
ike 0:to_HQ:101: sent IKE msg (quick_ilsend): 173.1.1.1:500->11.101.1.1:500, len=620,
id=df03f1d4820222a/6c2caf4dcf5bab75:32f4cc01
ike 0: comes 11.101.1.1:500->173.1.1.1:500,ifindex=42....
ike 0: IKEv1 exchange=Quick id=df03f1d4820222a/6c2caf4dcf5bab75:32f4cc01 len=444
ike 0:to_HQ:101:to_HQ:259: responder selectors 0:0.0.0.0/0.0.0.0:0->0:0.0.0.0/0.0.0.0:0
ike 0:to_HQ:101:to_HQ:259: my proposal:
ike 0:to_HQ:101:to_HQ:259: proposal id = 1:
ike 0:to_HQ:101:to_HQ:259: protocol id = IPSEC_ESP:
ike 0:to_HQ:101:to_HQ:259: PFS DH group = 14
ike 0:to_HQ:101:to_HQ:259: trans_id = ESP_AES_CBC (key_len = 128)
ike 0:to_HQ:101:to_HQ:259: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:to_HQ:101:to_HQ:259: type = AUTH_ALG, val=SHA1
ike 0:to_HQ:101:to_HQ:259: trans_id = ESP_AES_CBC (key_len = 256)
ike 0:to_HQ:101:to_HQ:259: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:to_HQ:101:to_HQ:259: type = AUTH_ALG, val=SHA1
ike 0:to_HQ:101:to_HQ:259: trans_id = ESP_AES_CBC (key_len = 128)
ike 0:to_HQ:101:to_HQ:259: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:to_HQ:101:to_HQ:259: type = AUTH_ALG, val=SHA2_256
ike 0:to_HQ:101:to_HQ:259: trans_id = ESP_AES_CBC (key_len = 256)
ike 0:to_HQ:101:to_HQ:259: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:to_HQ:101:to_HQ:259: type = AUTH_ALG, val=SHA2_256
ike 0:to_HQ:101:to_HQ:259: trans_id = ESP_AES_GCM_16 (key_len = 128)
ike 0:to_HQ:101:to_HQ:259: encapsulation = ENCAPSULATION_MODE_TUNNEL

```

```

ike 0:to_HQ:101:to_HQ:259: type = AUTH_ALG, val=NULL
ike 0:to_HQ:101:to_HQ:259: trans_id = ESP_AES_GCM_16 (key_len = 256)
ike 0:to_HQ:101:to_HQ:259: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:to_HQ:101:to_HQ:259: type = AUTH_ALG, val=NULL
ike 0:to_HQ:101:to_HQ:259: trans_id = ESP_CHACHA20_POLY1305 (key_len = 256)
ike 0:to_HQ:101:to_HQ:259: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:to_HQ:101:to_HQ:259: type = AUTH_ALG, val=NULL
ike 0:to_HQ:101:to_HQ:259: incoming proposal:
ike 0:to_HQ:101:to_HQ:259: proposal id = 1:
ike 0:to_HQ:101:to_HQ:259: protocol id = IPSEC_ESP:
ike 0:to_HQ:101:to_HQ:259: PFS DH group = 14
ike 0:to_HQ:101:to_HQ:259: trans_id = ESP_AES_CBC (key_len = 128)
ike 0:to_HQ:101:to_HQ:259: encapsulation = ENCAPSULATION_MODE_TUNNEL
ike 0:to_HQ:101:to_HQ:259: type = AUTH_ALG, val=SHA1
ike 0:to_HQ: schedule auto-negotiate
ike 0:to_HQ:101:to_HQ:259: replay protection enabled
ike 0:to_HQ:101:to_HQ:259: SA life soft seconds=42902.
ike 0:to_HQ:101:to_HQ:259: SA life hard seconds=43200.
ike 0:to_HQ:101:to_HQ:259: IPsec SA selectors #src=1 #dst=1
ike 0:to_HQ:101:to_HQ:259: src 0 4 0:0.0.0.0/0.0.0.0:0
ike 0:to_HQ:101:to_HQ:259: dst 0 4 0:0.0.0.0/0.0.0.0:0
ike 0:to_HQ:101:to_HQ:259: add IPsec SA: SPIs=ca64644b/747c10c9
ike 0:to_HQ:101:to_HQ:259: IPsec SA dec spi ca64644b key
16:D5C60F1A3951B288CE4DEC7E04D2119D auth 20:F872A7A26964208A9AA368A31AEFA3DB3F3780BC
ike 0:to_HQ:101:to_HQ:259: IPsec SA enc spi 747c10c9 key
16:97952E1594F718128D9D7B09400856EA auth 20:4D5E5BC45A9D5A9A4631E911932F5650A4639A37
ike 0:to_HQ:101:to_HQ:259: added IPsec SA: SPIs=ca64644b/747c10c9
ike 0:to_HQ:101:to_HQ:259: sending SNMP tunnel UP trap
ike 0:to_HQ:101: sent IKE msg (quick_i2send): 173.1.1.1:500->11.101.1.1:500, len=76,
id=dfdf03f1d4820222a/6c2caf4dcf5bab75:32f4cc01

```

## SSL VPN

The following topics provide information about SSL VPN:

- [SSL VPN best practices on page 1370](#)
- [SSL VPN quick start on page 1373](#)
- [SSL VPN tunnel mode on page 1380](#)
- [SSL VPN web mode for remote user on page 1386](#)
- [SSL VPN authentication on page 1391](#)
- [SSL VPN to IPsec VPN on page 1469](#)
- [SSL VPN protocols on page 1479](#)
- [SSL VPN troubleshooting on page 1480](#)
- [Restricting VPN access to rogue/non-compliant devices with Security Fabric](#)

## SSL VPN best practices

Securing remote access to network resources is a critical part of security operations. SSL VPN allows administrators to configure, administer, and deploy a remote access strategy for their remote workers.



Choosing the correct mode of operation and applying the proper levels of security are integral to providing optimal performance and user experience, and keeping your user data safe.

The below guidelines outline selecting the correct SSL VPN mode for your deployment and employing best practices to ensure that your data are protected.

Information about SSL VPN throughput and maximum concurrent users is available on your device's datasheet; see [Next-Generation Firewalls Models and Specifications](#).

## Tunnel mode

In tunnel mode, the SSL VPN client encrypts all traffic from the remote client computer and sends it to the FortiGate through an SSL VPN tunnel over the HTTPS link between the user and the FortiGate.

The FortiGate establishes a tunnel with the client, and assigns a virtual IP (VIP) address to the client from a range reserved addresses. While the underlying protocols are different, the outcome is very similar to a IPsec VPN tunnel. All client traffic is encrypted, allowing the users and networks to exchange a wide range of traffic, regardless of the application or protocols.

Use this mode if you require:

- A wide range of applications and protocols to be accessed by the remote client.
- No proxying is done by the FortiGate.
- Straightforward configuration and administration, as traffic is controlled by firewall policies.
- A transparent experience for the end user. For example, a user that needs to RDP to their server only requires a tunnel connection; they can then use the usual client application, like Windows Remote Desktop, to connect.

Full tunneling forces all traffic to pass through the FortiGate (see [SSL VPN full tunnel for remote user on page 1380](#)).

Split tunneling only routes traffic to the designated network through the FortiGate (see [SSL VPN split tunnel for remote user on page 1373](#)).

## Limitations

Tunnel mode requires that the [FortiClient VPN](#) client be installed on the remote end. The standalone FortiClient VPN client is free to use, and can accommodate SSL VPN and IPsec VPN tunnels. For supported operating systems, see the [FortiClient Technical Specifications](#).

## Web mode

Web-only mode provides clientless network access using a web browser with built-in SSL encryption. Users authenticate to FortiGate's SSL VPN Web Portal, which provides access to network services and resources, including HTTP/HTTPS, Telnet, FTP, SMB/CIFS, VNC, RDP, and SSH. When a user starts a connection to a server from the web portal, FortiOS proxies this communication with the server. All communication between the FortiGate and the user continues to be over HTTPS, regardless of the service that is being accessed.

Use this mode if you require:

- A clientless solution in which all remote services are access through a web portal.
- Tight control over the contents of the web portal.
- Limited services provided to the remote users.

## Limitations

- Multiple applications and protocols are not supported.
- VNC and RDP access might have limitations, such as certain shortcut keys not being supported.
- In some configurations RDP can consume a significant amount of memory and CPU time.
- Firewall performance might decrease as remote usage increases.
- Highly customized web pages might not render correctly.

## Security best practices

### Integrate with authentication servers

For networks with many users, integrate your user configuration with existing authentication servers through LDAP, RADIUS, or FortiAuthenticator.

By integrating with existing authentication servers, such as Windows AD, there is a lower change of making mistakes when configuring local users and user groups. Your administration effort is also reduces.

See [SSL VPN with LDAP user authentication on page 1391](#) for more information.

### Use a non-factory SSL certificate for the SSL VPN portal

Your certificate should identify your domain so that a remote user can recognize the identity of the server or portal that they are accessing through a trusted CA.

The default Fortinet factory self-signed certificates are provided to simplify initial installation and testing. If you use these certificates you are vulnerable to man-in-the-middle attacks, where an attacker spoofs your certificate, compromises your connection, and steals your personal information. It is highly recommended that you purchase a server certificate from a trusted CA to allow remote users to connect to SSL VPN with confidence. See [Procure and import a signed SSL certificate on page 741](#) for more information.

Enabling the *Do not Warn Invalid Server Certificate* option on the client disables the certificate warning message, potentially allowing users to accidentally connect to untrusted servers. Disabling invalid server certificate warnings is not recommended.

### Use multi-factor authentication

Multi-factor authentication (MFA) ensures that the end-user is who they claim to be by requiring at least two factors - a piece of information that the user knows (password), and an asset that the user has (OTP). A third factor, something a user is (fingerprint or face), may be enabled as well. [FortiToken Mobile](#) is typically used for MFA.

FortiGate comes with two free FortiTokens, and more can be purchased from the [FortiToken Mobile iOS app](#) or through Fortinet partners.

See [SSL VPN with FortiToken mobile push authentication on page 1413](#) for more information.

2FA, a subset of MFA, can also be set up with email tokens. See [Email Two-Factor Authentication on FortiGate](#) for information.

### Deploy user certificates for remote SSL VPN users

This method of 2FA uses a user certificate as the second authentication factor. This is more secure, as it identifies the end user using a certificate. The configuration and administration of this solution is significantly more complicated, and

requires administrators with advanced knowledge of the FortiGate and certificate deployment.

See [SSL VPN with certificate authentication on page 1450](#) for more information.

### Define your minimum supported TLS version and cipher suites

Minimum and maximum supported TLS version can be configured in the FortiGate CLI. The cipher algorithm can also be customized.

See [How to control the SSL version and cipher suite for SSL VPN](#) for more information.

### Properly administer firewall policies and profiles against only the access level required for the remote user

Users do not all require the same access. Access should only be granted after careful considerations. Typically, users are placed in groups, and each group is allowed access to limited resources.

Using SSL VPN realms simplifies defining the control structure for mapping users and groups to the appropriate resources.

See [SSL VPN multi-realm on page 1464](#) for more information.

## SSL VPN quick start

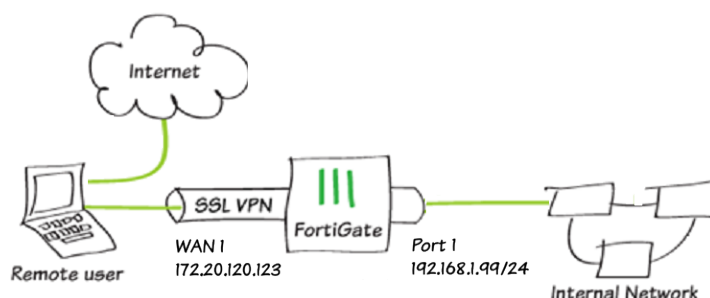
The following topics provide introductory instructions on configuring SSL VPN:

- [SSL VPN split tunnel for remote user on page 1373](#)
- [Connecting from FortiClient VPN client on page 1376](#)
- [Set up FortiToken multi-factor authentication on page 1378](#)
- [Connecting from FortiClient with FortiToken on page 1379](#)

### SSL VPN split tunnel for remote user

This is a sample configuration of remote users accessing the corporate network and internet through an SSL VPN by tunnel mode using FortiClient but accessing the Internet without going through the SSL VPN tunnel.

#### Sample topology



## Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface.



The split tunneling routing address cannot use an FQDN or an address group that includes an FQDN.

### To configure SSL VPN using the GUI:

1. Configure the interface and firewall address. The port1 interface connects to the internal network.
  - a. Go to *Network > Interfaces* and edit the *wan1* interface.
  - b. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.
  - c. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.
  - d. Click *OK*.
  - e. Go to *Policy & Objects > Address* and create an address for internal subnet *192.168.1.0*.
2. Configure user and user group.
  - a. Go to *User & Device > User Definition* to create a local user *sslvpnuser1*.
  - b. Go to *User & Device > User Groups* to create a group *sslvpngroup* with the member *sslvpnuser1*.
3. Configure SSL VPN web portal.
  - a. Go to *VPN > SSL-VPN Portals* to create a tunnel mode only portal *my-split-tunnel-portal*.
  - b. Enable *Split Tunneling*.
  - c. Select *Routing Address* to define the destination network that will be routed through the tunnel. Leave undefined to use the destination in the respective firewall policies.
4. Configure SSL VPN settings.
  - a. Go to *VPN > SSL-VPN Settings*.
  - b. For *Listen on Interface(s)*, select *wan1*.
  - c. Set *Listen on Port* to *10443*.
  - d. Optionally, set *Restrict Access* to *Limit access to specific hosts*, and specify the addresses of the hosts that are allowed to connect to this VPN.
  - e. Choose a certificate for *Server Certificate*. The default is *Fortinet\_Factory*.
  - f. In *Authentication/Portal Mapping All Other Users/Groups*, set the *Portal* to *tunnel-access*.
  - g. Create new *Authentication/Portal Mapping* for group *sslvpngroup* mapping portal *my-split-tunnel-portal*.
5. Configure SSL VPN firewall policy.
  - a. Go to *Policy & Objects > IPv4 Policy*.
  - b. Fill in the firewall policy name. In this example, *sslvpn split tunnel access*.
  - c. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.
  - d. Choose an *Outgoing Interface*. In this example, *port1*.
  - e. Set the *Source* to *SSLVPN\_TUNNEL\_ADDR1* and group to *sslvpngroup*. The source address references the tunnel IP addresses that the remote clients are using.
  - f. In this example, the *Destination* is *192.168.1.0*.
  - g. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.
  - h. Click *OK*.

**To configure SSL VPN using the CLI:****1. Configure the interface and firewall address.**

```
config system interface
 edit "wan1"
 set vdom "root"
 set ip 172.20.120.123 255.255.255.0
 next
end
```

**2. Configure internal interface and protected subnet, then connect the port1 interface to the internal network.**

```
config system interface
 edit "port1"
 set vdom "root"
 set ip 192.168.1.99 255.255.255.0
 next
end

config firewall address
 edit "192.168.1.0"
 set subnet 192.168.1.0 255.255.255.0
 next
end
```

**3. Configure user and user group.**

```
config user local
 edit "sslvpnuser1"
 set type password
 set passwd your-password
 next
end

config user group
 edit "sslvpngroup"
 append member "sslvpnuser1"
 next
end
```

**4. Configure SSL VPN web portal.**

```
config vpn ssl web portal
 edit "my-split-tunnel-portal"
 set tunnel-mode enable
 set split-tunneling enable
 set split-tunneling-routing-address "192.168.1.0"
 set ip-pools "SSLVPN_TUNNEL_ADDR1"
 next
end
```

**5. Configure SSL VPN settings.**

```
config vpn ssl settings
 set servercert "Fortinet_Factory"
 set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
 set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
 set source-interface "wan1"
 set source-address "all"
```

```
set source-address6 "all"
set default-portal "full-access"
config authentication-rule
 edit 1
 set groups "sslvpngroup"
 set portal "my-split-tunnel-portal"
 next
next
end
```

Optionally, to restrict access to specific hosts:

```
config vpn ssl settings
 set source-address <address> <address> ... <address>
 set source-address6 <address> <address> ... <address>
end
```

6. Configure one SSL VPN firewall policy to allow remote user to access the internal network. Traffic is dropped from internal to remote client.

```
config firewall policy
 edit 1
 set name "sslvpn split tunnel access"
 set srcintf "ssl.root"
 set dstintf "port1"
 set srcaddr "SSLVPN_TUNNEL_ADDR1"
 set dstaddr "192.168.1.0"
 set groups "sslvpngroup"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end
```

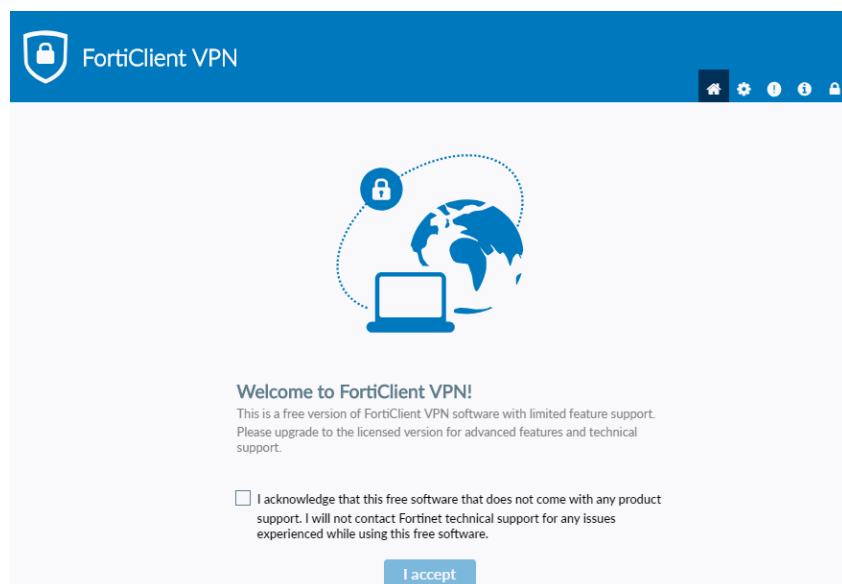
## Connecting from FortiClient VPN client

For FortiGate administrators, a free version of FortiClient VPN is available which supports basic IPsec and SSL VPN and does not require registration with EMS. This version does not include central management, technical support, or some advanced features.

### Downloading and installing the standalone FortiClient VPN client

You can download the free VPN client from [FNDN](#) or [FortiClient.com](#).

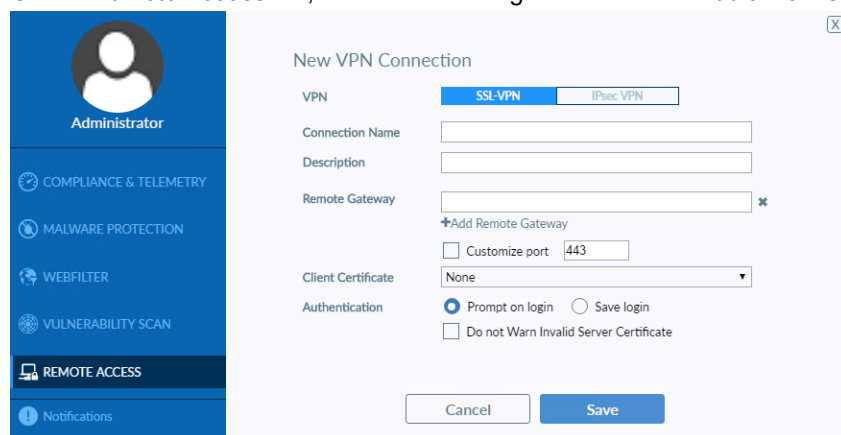
When the free VPN client is run for the first time, it displays a disclaimer. You cannot configure or create a VPN connection until you accept the disclaimer and click *I accept*:



## Configuring an SSL VPN connection

### To configure an SSL VPN connection:

1. On the *Remote Access* tab, click on the settings icon and then *Add a New Connection*.



2. Select *SSL-VPN*, then configure the following settings:

<b>Connection Name</b>	SSLVPNtoHQ
<b>Description</b>	(Optional)
<b>Remote Gateway</b>	172.20.120.123
<b>Customize port</b>	10443
<b>Client Certificate</b>	Select <i>Prompt on connect</i> or the certificate from the dropdown list.
<b>Authentication</b>	Select <i>Prompt on login</i> for a prompt on the connection screen

3. Click *Save* to save the VPN connection.

## Connecting to SSL VPN

### To connect to SSL VPN:

1. On the *Remote Access* tab, select the VPN connection from the dropdown list.  
Optionally, you can right-click the FortiTray icon in the system tray and select a VPN configuration to connect.
2. Enter your username and password.
3. Click the *Connect* button.
4. After connecting, you can now browse your remote network. Traffic to 192.168.1.0 goes through the tunnel, while other traffic goes through the local gateway. FortiClient displays the connection status, duration, and other relevant information.
5. Click the *Disconnect* button when you are ready to terminate the VPN session.

## Checking the SSL VPN connection

### To check the SSL VPN connection using the GUI:

1. On the FortiGate, go to *VPN > Monitor > SSL-VPN Monitor* to verify the list of SSL users.
2. On the FortiGate, go to *Log & Report > Forward Traffic* to view the details of the SSL entry.

### To check the tunnel log in using the CLI:

```
get vpn ssl monitor
SSL VPN Login Users:
```

Index	User	Auth Type	Timeout	From	HTTP in/out	HTTPS in/out
0	sslvpnuser1	1 (1)	291	10.1.100.254	0/0	0/0

```
SSL VPN sessions:
```

Index	User	Source IP	Duration	I/O Bytes	Tunnel/Dest IP
0	sslvpnuser1	10.1.100.254	9	22099/43228	10.212.134.200

## Set up FortiToken multi-factor authentication

This configuration adds multi-factor authentication (MFA) to the split tunnel configuration ([SSL VPN split tunnel for remote user on page 1373](#)). It uses one of the two free mobile FortiTokens that is already installed on the FortiGate.

### To configure MFA using the GUI:

1. Configure the user:
  - a. Go to *User & Device > User Definition* and edit local user *sslvpnuser1*.
  - b. Enter the user's *Email Address*.
  - c. Enable *Two-factor Authentication* and select one mobile *Token* from the list,
  - d. Enable *Send Activation Code* and select *Email*.
  - e. Click *Next* and click *Submit*.
2. Activate the mobile token:
  - a. When a FortiToken is added to user *sslvpnuser1*, an email is sent to the user's email address. Follow the instructions to install your FortiToken mobile application on your device and activate your token.



## To configure MFA using the CLI:

### 1. Configure the user:

```
config user local
 edit "sslvpnuser1"
 set type password
 set two-factor fortitoken
 set fortitoken <select mobile token for the option list>
 set email-to <user's email address>
 set passwd <user's password>
 next
end
```

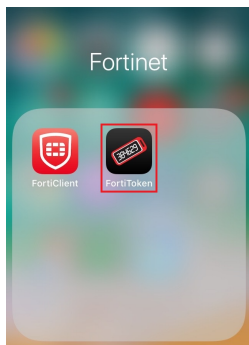
### 2. Activate the mobile token:

- a. When a FortiToken is added to user *sslvpnuser1*, an email is sent to the user's email address. Follow the instructions to install your FortiToken mobile application on your device and activate your token.

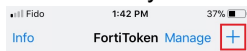
## Connecting from FortiClient with FortiToken

### To activate your FortiToken:

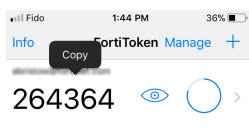
1. On your device, open FortiToken Mobile. If this is your first time opening the application, it may prompt you to create a PIN for secure access to the application and tokens.



2. You should have received your notification via email, select + and use the device camera to scan the token QR code in your email.



3. FortiToken Mobile provisions and activates your token and generates token codes immediately. To view the OTP's digits, select the eye icon. After you open the application, FortiToken Mobile generates a new six-digit OTP every 30 seconds.



### To connect to SSL VPN:

1. On the *Remote Access* tab, select the VPN connection from the dropdown list. Optionally, you can right-click the FortiTray icon in the system tray and select a VPN configuration to connect.
2. Enter your username and password.
3. Click the *Connect* button.

4. A Token field will appear, prompting you for the FortiToken code. Enter the FortiToken code from your Mobile device.
5. After connecting, you can now browse your remote network. Traffic to 192.168.1.0 goes through the tunnel, while other traffic goes through the local gateway. FortiClient displays the connection status, duration, and other relevant information.
6. Click the *Disconnect* button when you are ready to terminate the VPN session.

## SSL VPN tunnel mode

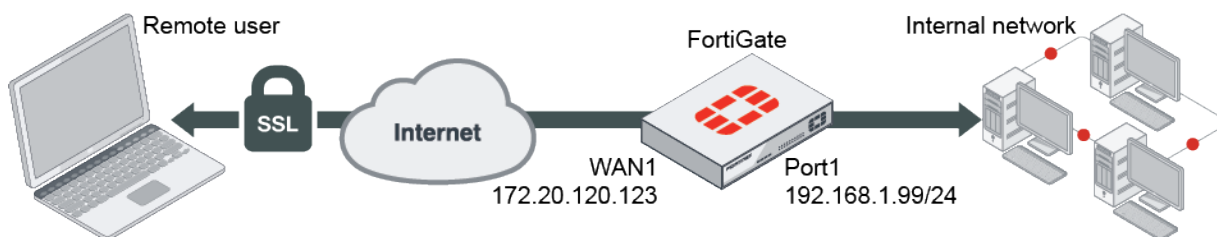
The following topics provide instructions on configuring SSL VPN tunnel mode:

- [SSL VPN full tunnel for remote user](#)
- [SSL VPN tunnel mode host check](#)

### SSL VPN full tunnel for remote user

This is a sample configuration of remote users accessing the corporate network and internet through an SSL VPN by tunnel mode using FortiClient.

#### Sample topology



#### Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface.

#### To configure SSL VPN using the GUI:

1. Configure the interface and firewall address:
  - a. Go to *Network > Interfaces* and edit the *wan1* interface.
  - b. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.
  - c. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.
  - d. Click *OK*.
2. Configure user and user group:
  - a. Go to *User & Device > User Definition* to create a local user *sslvpnuser1*.
  - b. Go to *User & Device > User Groups* to create a group *sslvpngroup* with the member *sslvpnuser1*.
3. Configure SSL VPN web portal:
  - a. Go to *VPN > SSL-VPN Portals* to create a tunnel mode only portal *my-full-tunnel-portal*.
  - b. Disable *Split Tunneling*.

4. Configure SSL VPN settings:
  - a. Go to *VPN > SSL-VPN Settings*.
  - b. For *Listen on Interface(s)*, select *wan1*.
  - c. Set *Listen on Port* to *10443*.
  - d. Optionally, set *Restrict Access* to *Limit access to specific hosts*, and specify the addresses of the hosts that are allowed to connect to this VPN.
  - e. Choose a certificate for *Server Certificate*. The default is *Fortinet\_Factory*.
  - f. In *Authentication/Portal Mapping All Other Users/Groups*, set the *Portal* to *tunnel-access*.
  - g. Create new *Authentication/Portal Mapping* for group *sslvpngroup* mapping portal *my-full-tunnel-portal*.
5. Configure SSL VPN firewall policies to allow remote user to access the internal network:
  - a. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
  - b. Set *Name* to *sslvpn tunnel mode access*.
  - c. Set *Incoming Interface* to *SSL-VPN tunnel interface(ssl.root)*.
  - d. Set *Outgoing Interface* to *port1*.
  - e. Set the *Source Address* to *SSLVPN\_TUNNEL\_ADDR1* and *User* to *sslvpngroup*. The source address references the tunnel IP addresses that the remote clients are using.
  - f. Set *Destination* to *all*, *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.
  - g. Click *OK*.
  - h. Click *Create New*.
  - i. Set *Name* to *sslvpn tunnel mode outgoing*.
  - j. Configure the same settings as the previous policy, except set *Outgoing Interface* to *wan1*.
  - k. Click *OK*.

### To configure SSL VPN using the CLI:

1. Configure the interface and firewall address:

```
config system interface
 edit "wan1"
 set vdom "root"
 set ip 172.20.120.123 255.255.255.0
 next
end
```

2. Configure the internal interface and protected subnet, then connect the port1 interface to the internal network:

```
config system interface
 edit "port1"
 set vdom "root"
 set ip 192.168.1.99 255.255.255.0
 next
end
```

3. Configure user and user group:

```
config user local
 edit "sslvpnuser1"
 set type password
 set passwd your-password
 next
end
```

```

config user group
 edit "sslvpngroup"
 set member "vpnuser1"
 next
end

```

#### 4. Configure SSL VPN web portal and predefine RDP bookmark for windows server:

```

config vpn ssl web portal
 edit "my-full-tunnel-portal"
 set tunnel-mode enable
 set split-tunneling disable
 set ip-pools "SSLVPN_TUNNEL_ADDR1"
 next
end

```

#### 5. Configure SSL VPN settings:

```

config vpn ssl settings
 set servercert "Fortinet_Factory"
 set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
 set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
 set source-interface "wan1"
 set source-address "all"
 set source-address6 "all"
 set default-portal "full-access"
 config authentication-rule
 edit 1
 set groups "sslvpngroup"
 set portal "my-full-tunnel-portal"
 next
 end
end

```

Optionally, to restrict access to specific hosts:

```

config vpn ssl settings
 set source-address <address> <address> ... <address>
 set source-address6 <address> <address> ... <address>
end

```

#### 6. Configure SSL VPN firewall policies to allow remote user to access the internal network. Traffic is dropped from internal to remote client.

```

config firewall policy
 edit 1
 set name "sslvpn tunnel mode access"
 set srcintf "ssl.root"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "all"
 set groups "sslvpngroup"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set name "sslvpn tunnel mode outgoing"
 set srcintf "ssl.root"

```

```

 set dstintf "wan1"
 set srcaddr "all"
 set dstaddr "all"
 set groups "sslvpngroup"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end

```

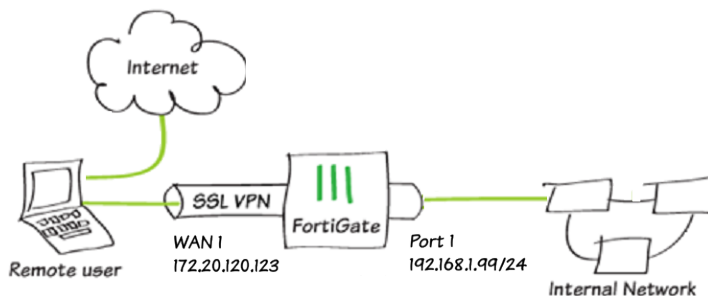
### To see the results:

1. Download FortiClient from [www.forticlient.com](http://www.forticlient.com).
2. Open the FortiClient Console and go to *Remote Access*.
3. Add a new connection.
  - Set *VPN Type* to *SSL VPN*.
  - Set *Remote Gateway* to the IP of the listening FortiGate interface, in this example, *172.20.120.123*.
4. Select *Customize Port* and set it to *10443*.
5. Save your settings.
6. Use the credentials you've set up to connect to the SSL VPN tunnel.
7. After connection, all traffic except the local subnet will go through the tunnel *FGT*.
8. Go to *VPN > Monitor > SSL-VPN Monitor* to verify the list of SSL users.
9. On the FortiGate, go to *Log & Report > Forward Traffic* and view the details for the SSL entry.

## SSL VPN tunnel mode host check

This is a sample configuration of remote users accessing the corporate network through an SSL VPN by tunnel mode using FortiClient with AV host check.

### Sample topology



### Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface.



The split tunneling routing address cannot use an FQDN or an address group that includes an FQDN.

### To configure SSL VPN using the GUI:

1. Configure the interface and firewall address. The port1 interface connects to the internal network.
  - a. Go to *Network > Interfaces* and edit the *wan1* interface.
  - b. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.
  - c. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.
  - d. Click OK.
  - e. Go to *Policy & Objects > Address* and create an address for internet subnet *192.168.1.0*.
2. Configure user and user group.
  - a. Go to *User & Device > User Definition* to create a local user *sslvpnuser1*.
  - b. Go to *User & Device > User Groups* to create a group *sslvpngroup* with the member *sslvpnuser1*.
3. Configure SSL VPN web portal.
  - a. Go to *VPN > SSL-VPN Portals* to create a tunnel mode only portal *my-split-tunnel-portal*.
  - b. Enable *Tunnel Mode* and *Enable Split Tunneling*.
  - c. Select *Routing Address*.
4. Configure SSL VPN settings.
  - a. Go to *VPN > SSL-VPN Settings*.
  - b. For *Listen on Interface(s)*, select *wan1*.
  - c. Set *Listen on Port* to *10443*.
  - d. Choose a certificate for *Server Certificate*. The default is *Fortinet\_Factory*.
  - e. In *Authentication/Portal Mapping All Other Users/Groups*, set the *Portal* to *tunnel-access*.
  - f. Create new *Authentication/Portal Mapping* for group *sslvpngroup* mapping portal *my-split-tunnel-portal*.
5. Configure SSL VPN firewall policy.
  - a. Go to *Policy & Objects > IPv4 Policy*.
  - b. Fill in the firewall policy name. In this example, *sslvpn tunnel access with av check*.
  - c. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.
  - d. Choose an *Outgoing Interface*. In this example, *port1*.
  - e. Set the *Source* to *all* and group to *sslvpngroup*.
  - f. In this example, the *Destination* is *all*.
  - g. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.
  - h. Click OK.
6. Use CLI to configure SSL VPN web portal to enable the host to check for compliant antivirus software on the user's computer.

```
config vpn ssl web portal
 edit my-split-tunnel-access
 set host-check av
 next
end
```

### To configure SSL VPN using the CLI:

1. Configure the interface and firewall address.

```
config system interface
 edit "wan1"
 set vdom "root"
 set ip 172.20.120.123 255.255.255.0
```

```
 next
end
```

**2. Configure internal interface and protected subnet, then connect the port1 interface to the internal network.**

```
config system interface
 edit "port1"
 set vdom "root"
 set ip 192.168.1.99 255.255.255.0
 next
end

config firewall address
 edit "192.168.1.0"
 set subnet 192.168.1.0 255.255.255.0
 next
end
```

**3. Configure user and user group.**

```
config user local
 edit "sslvpnuser1"
 set type password
 set passwd your-password
 next
end

config user group
 edit "sslvpngroup"
 set member "vpnuser1"
 next
end
```

**4. Configure SSL VPN web portal.**

```
config vpn ssl web portal
 edit "my-split-tunnel-portal"
 set tunnel-mode enable
 set split-tunneling enable
 set split-tunneling-routing-address "192.168.1.0"
 set ip-pools "SSLVPN_TUNNEL_ADDR1"
 next
end
```

**5. Configure SSL VPN settings.**

```
config vpn ssl settings
 set servercert "Fortinet_Factory"
 set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
 set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
 set source-interface "wan1"
 set source-address "all"
 set source-address6 "all"
 set default-portal "full-access"
 config authentication-rule
 edit 1
 set groups "sslvpngroup"
 set portal "my-split-tunnel-portal"
 next
 end
end
```

```

 end
end

```

6. Configure one SSL VPN firewall policy to allow remote user to access the internal network. Traffic is dropped from internal to remote client.

```

config firewall policy
 edit 1
 set name "sslvpn web mode access"
 set srcintf "ssl.root"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "192.168.1.0"
 set groups "sslvpngroup"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end

```

7. Configure SSL VPN web portal to enable the host to check for compliant antivirus software on the user's computer:

```

config vpn ssl web portal
 edit my-split-tunnel-access
 set host-check av
 next
end

```

#### To see the results:

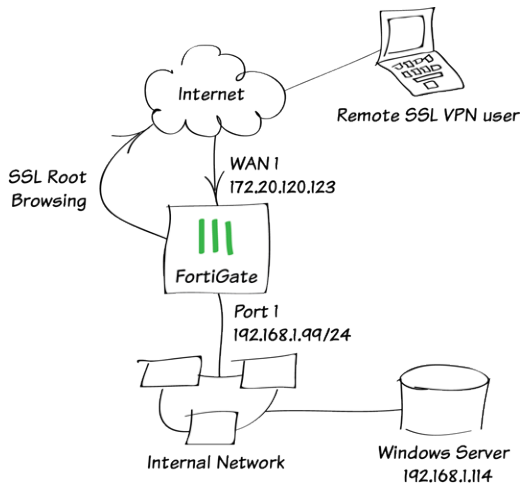
1. Download FortiClient from [www.forticlient.com](http://www.forticlient.com).
2. Open the FortiClient Console and go to *Remote Access*.
3. Add a new connection:
  - Set *VPN Type* to *SSL VPN*.
  - Set *Remote Gateway* to the IP of the listening FortiGate interface, in this example, *172.20.120.123*.
4. Select *Customize Port* and set it to *10443*.
5. Save your settings.
6. Use the credentials you've set up to connect to the SSL VPN tunnel.  
If the user's computer has antivirus software, a connection is established; otherwise FortiClient shows a compliance warning.
7. After connection, traffic to *192.168.1.0* goes through the tunnel. Other traffic goes through local gateway.
8. On the FortiGate, go to *VPN > Monitor > SSL-VPN Monitor* to verify the list of SSL users.
9. On the FortiGate, go to *Log & Report > Forward Traffic* and view the details for the SSL entry.

## SSL VPN web mode for remote user

This is a sample configuration of remote users accessing the corporate network through an SSL VPN by web mode using a web browser.



## Sample topology



## Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface.

### To configure SSL VPN using the GUI:

1. Configure the interface and firewall address. The port1 interface connects to the internal network.
  - a. Go to *Network > Interfaces* and edit the *wan1* interface.
  - b. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.
  - c. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.
  - d. Click OK.
  - e. Go to *Policy & Objects > Address* and create an address for internet subnet *192.168.1.0*.
2. Configure user and user group.
  - a. Go to *User & Device > User Definition* to create a local user *sslvpnuser1*.
  - b. Go to *User & Device > User Groups* to create a group *sslvpngroup* with the member *sslvpnuser1*.
3. Configure SSL VPN web portal.
  - a. Go to *VPN > SSL-VPN Portals* to create a web mode only portal *my-web-portal*.
  - b. Set *Predefined Bookmarks for Windows server* to type *RDP*.
4. Configure SSL VPN settings.
  - a. Go to *VPN > SSL-VPN Settings*.
  - b. For *Listen on Interface(s)*, select *wan1*.
  - c. Set *Listen on Port* to *10443*.
  - d. Choose a certificate for *Server Certificate*. The default is *Fortinet\_Factory*.
  - e. In *Authentication/Portal Mapping All Other Users/Groups*, set the *Portal* to *web-access*.
  - f. Create new *Authentication/Portal Mapping* for group *sslvpngroup* mapping portal *my-Web-portal*.
5. Configure SSL VPN firewall policy.
  - a. Go to *Policy & Objects > IPv4 Policy*.
  - b. Fill in the firewall policy name. In this example, *sslvpn web mode access*.

- c. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.
- d. Choose an *Outgoing Interface*. In this example, *port1*.
- e. Set the *Source* to *all* and group to *sslvpngroup*.
- f. In this example, the *Destination* is the internal protected subnet *192.168.1.0*.
- g. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.
- h. Click *OK*.

### To configure SSL VPN using the CLI:

1. Configure the interface and firewall address.

```
config system interface
 edit "wan1"
 set vdom "root"
 set ip 172.20.120.123 255.255.255.0
 next
end
```

2. Configure the internal interface and protected subnet, then connect the port1 interface to the internal network.

```
config system interface
 edit "port1"
 set vdom "root"
 set ip 192.168.1.99 255.255.255.0
 next
end

config firewall address
 edit "192.168.1.0"
 set subnet 192.168.1.0 255.255.255.0
 next
end
```

3. Configure user and user group.

```
config user local
 edit "sslvpnuser1"
 set type password
 set passwd your-password
 next
end

config user group
 edit "sslvpngroup"
 set member "vpnuser1"
 next
end
```

4. Configure SSL VPN web portal and predefine RDP bookmark for windows server.

```
config vpn ssl web portal
 edit "my-web-portal"
 set web-mode enable
 config bookmark-group
 edit "gui-bookmarks"
 config bookmarks
 edit "Windows Server"
 set apptype rdp
 next
 next
 next
 next
end
```

```

 set host "192.168.1.114"
 set port 3389
 set logon-user "your-windows-server-user-name"
 set logon-password your-windows-server-password
 next
end
next
end
next
end

```

## 5. Configure SSL VPN settings.

```

config vpn ssl settings
 set servercert "Fortinet_Factory"
 set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
 set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
 set source-interface "wan1"
 set source-address "all"
 set source-address6 "all"
 set default-portal "full-access"
 config authentication-rule
 edit 1
 set groups "sslvpngroup"
 set portal "my-web-portal"
 next
 end
end

```

## 6. Configure one SSL VPN firewall policy to allow remote user to access the internal network. Traffic is dropped from internal to remote client

```

config firewall policy
 edit 1
 set name "sslvpn web mode access"
 set srcintf "ssl.root"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "192.168.1.0"
 set groups "sslvpngroup"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end

```

### To see the results:

1. In a web browser, log into the portal <https://172.20.120.123:10443> using the credentials you've set up.
2. In the portal with the predefined bookmark, select the bookmark to begin an RDP session. If there are no predefined bookmarks, the Quick Connection tool can be used; see [Quick Connection tool on page 1390](#) for more information.
3. Go to *VPN > Monitor > SSL-VPN Monitor* to verify the list of SSL users.
4. Go to *Log & Report > Forward Traffic* to view the details for the SSL entry.

## Quick Connection tool

The Quick Connection tool allows a user to connect to a resource when it is not a predefined bookmark. The tool allows the user to specify the type of server and the URL or IP address of the host.

### To connect to a resource:

1. Select the connection type.
2. Enter the required information, such as the IP address or URL of the host.
3. Click *Launch*.



In a VNC session, to send Ctrl+Alt+Del, press *F8* then select *Send Ctrl-Alt-Delete*.

## RDP sessions



Some Windows servers require that a specific security be set for RDP sessions, as opposed to the standard RDP encryption security. For example, Windows 10 requires that TLS be used.

You can specify a location option if the remote computer does not use the same keyboard layout as your computer by appending it to the *Host* field using the following format: <IP address> -m <locale>

The available options are:

ar	Arabic	fr-be	Belgian French	no	Norwegian
da	Danish	fr-ca	Canadian French	pl	Polish
de	German	fr-ch	Swiss French	pt	Portuguese
de-ch	Swiss German	hr	Croatian	pt-br	Brazilian Portuguese
en-gb	British English	hu	Hungarian	ru	Russian
en-uk	UK English	it	Italian	sl	Slovenian
en-us	US English	ja	Japanese	sv	Sudanese

es	Spanish	lt	Lithuanian	tk	Turkmen
fi	Finnish	lv	Latvian	tr	Turkish
fr	French	mk	Macedonian		

## SSL VPN authentication

The following topics provide instructions on configuring SSL VPN authentication:

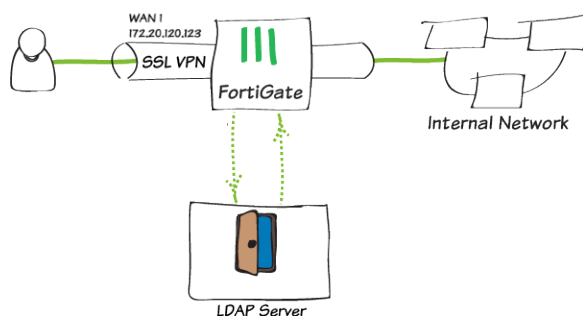
- [SSL VPN with LDAP user authentication on page 1391](#)
- [SSL VPN with LDAP user password renew on page 1396](#)
- [SSL VPN with LDAP-integrated certificate authentication on page 1401](#)
- [SSL VPN for remote users with MFA and user case sensitivity on page 1406](#)
- [SSL VPN with FortiToken mobile push authentication on page 1413](#)
- [SSL VPN with RADIUS on FortiAuthenticator on page 1418](#)
- [SSL VPN with RADIUS and FortiToken mobile push on FortiAuthenticator on page 1423](#)
- [SSL VPN with RADIUS password renew on FortiAuthenticator on page 1427](#)
- [SSL VPN with RADIUS on Windows NPS on page 1431](#)
- [SSL VPN with multiple RADIUS servers on page 1436](#)
- [SSL VPN with local user password policy on page 1445](#)
- [SSL VPN with certificate authentication on page 1450](#)
- [Dynamic address support for SSL VPN policies on page 1455](#)
- [SSL VPN multi-realm on page 1464](#)
- [SSL VPN with Azure AD SSO integration on page 1469](#)

## SSL VPN with LDAP user authentication

This is a sample configuration of SSL VPN for LDAP users. In this example, the LDAP server is a Windows 2012 AD server. A user *ldu1* is configured on Windows 2012 AD server.

You must have generated and exported a CA certificate from the AD server and then have imported it as an external CA certificate into the FortiGate.

### Sample topology



## Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface.

### To configure SSL VPN using the GUI:

1. Configure the interface and firewall address. The port1 interface connects to the internal network:
  - a. Go to *Network > Interfaces* and edit the *wan1* interface.
  - b. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.
  - c. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.
  - d. Click OK.
  - e. Go to *Policy & Objects > Address* and create an address for internet subnet *192.168.1.0*.
2. Import CA certificate into FortiGate:
  - a. Go to *System > Features Visibility* and ensure *Certificates* is enabled.
  - b. Go to *System > Certificates* and select *Import > CA Certificate*.
  - c. Select *Local PC* and then select the certificate file.  
The CA certificate now appears in the list of *External CA Certificates*. In this example, it is called *CA\_Cert\_1*.
  - d. If you want, you can use CLI commands to rename the system-generated *CA\_Cert\_1* to be more descriptive:

```
config vpn certificate ca
 rename CA_Cert_1 to LDAPS-CA
end
```
3. Configure the LDAP user:
  - a. Go to *User & Device > LDAP Servers* and click *Create New*.
  - b. Specify *Name* and *Server IP/Name*.
  - c. Specify *Common Name Identifier* and *Distinguished Name*.
  - d. Set *Bind Type* to *Regular*.
  - e. Specify *Username* and *Password*.
  - f. Enable *Secure Connection* and set *Protocol* to *LDAPS*.
  - g. For *Certificate*, select *LDAP server CA LDAPS-CA* from the list.
  - h. Click OK.
4. Configure user group:
  - a. Go to *User & Device > User Groups* to create a user group.
  - b. Enter a *Name*.
  - c. In *Remote Groups*, click *Add* to add *ldaps-server*.
5. Configure SSL VPN web portal:
  - a. Go to *VPN > SSL-VPN Portals* to edit the *full-access* portal.  
This portal supports both web and tunnel mode.
  - b. Disable *Enable Split Tunneling* so that all SSL VPN traffic goes through the FortiGate.
6. Configure SSL VPN settings:
  - a. Go to *VPN > SSL-VPN Settings*.
  - b. Select the *Listen on Interface(s)*, in this example, *wan1*.
  - c. Set *Listen on Port* to *10443*.
  - d. Set *Server Certificate* to the authentication certificate.
  - e. Under *Authentication/Portal Mapping*, set default Portal *web-access* for *All Other Users/Groups*.
  - f. Create new *Authentication/Portal Mapping* for group *ldaps-group* mapping portal *full-access*.

7. Configure SSL VPN firewall policy:
  - a. Go to *Policy & Objects > IPv4 Policy*.
  - b. Fill in the firewall policy name, in this example, *sslvpn certificate auth*.
  - c. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.
  - d. Set the *Source Address* to *all* and *Source User* to *ldaps-group*.
  - e. Set the *Outgoing Interface* to the local network interface so that the remote user can access the internal network, in this example, *port1*.
  - f. Set *Destination Address* to the internal protected subnet *192.168.1.0*.
  - g. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.
  - h. Enable *NAT*.
  - i. Configure any remaining firewall and security options as desired.
  - j. Click *OK*.

### To configure SSL VPN using the CLI:

1. Configure the interface and firewall address:

```
config system interface
 edit "wan1"
 set vdom "root"
 set ip 172.20.120.123 255.255.255.0
 next
end
```

2. Configure internal interface and protected subnet, then connect the port1 interface to the internal network:

```
config system interface
 edit "port1"
 set vdom "root"
 set ip 192.168.1.99 255.255.255.0
 next
end

config firewall address
 edit "192.168.1.0"
 set subnet 192.168.1.0 255.255.255.0
 next
end
```

3. Import CA certificate into FortiGate:

- a. Go to *System > Features Visibility* and ensure *Certificates* is enabled.
- b. Go to *System > Certificates* and select *Import > CA Certificate*.
- c. Set *Type* to *File*.
- d. Click *Upload* and find and select the certificate file.
- e. Click *OK*.  
The CA certificate now appears in the list of *External CA Certificates*. In this example, it is called *CA\_Cert\_1*.
- f. If you want, you can use CLI commands to rename the system-generated *CA\_Cert\_1* to be more descriptive:

```
config vpn certificate ca
 rename CA_Cert_1 to LDAPS-CA
end
```

**4. Configure the LDAP server:**

```
config user ldap
 edit "ldaps-server"
 set server "172.20.120.161"
 set cnid "cn"
 set dn "cn=Users,dc=qa,dc=fortinet,dc=com"
 set type regular
 set username "CN=Administrator,cn=users,DC=qa,DC=fortinet,DC=com"
 set password *****
 set group-member-check group-object
 set secure ldaps
 set ca-cert "LDAPS-CA"
 set port 636
 next
end
```

**5. Add the LDAP user to the user group:**

```
config user group
 edit "ldaps-group"
 append member "ldaps-server"
 next
end
```

**6. Configure SSL VPN web portal:**

```
config vpn ssl web portal
 edit "full-access"
 set tunnel-mode enable
 set web-mode enable
 set ip-pools "SSLVPN_TUNNEL_ADDR1"
 set split-tunneling disable
 next
end
```

**7. Configure SSL VPN settings:**

```
config vpn ssl settings
 set servercert "server_certificate"
 set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
 set source-interface "wan1"
 set source-address "all"
 set default-portal "web-access"
 config authentication-rule
 edit 1
 set groups "ldaps-group"
 set portal "full-access"
 next
 end
end
```

**8. Configure one SSL VPN firewall policy to allow remote user to access the internal network:**

```
config firewall policy
 edit 1
 set name "sslvpn web mode access"
 set srcintf "ssl.root"
 set dstintf "port1"
 set srcaddr "all"
```



```

 set dstaddr "192.168.1.0"
 set groups "ldaps-group"
 set action accept
 set schedule "always"
 set service "ALL"
 set nat enable
 next
end

```

### To see the results of web portal:

1. From a remote device, use a web browser to log into the SSL VPN web portal <http://172.20.120.123:10443>.
2. Enter the *ldu1* user credentials, then click *Login*.
3. Go to *VPN > Monitor > SSL-VPN Monitor* to verify the user's connection.

### To see the results of tunnel connection:

1. Download FortiClient from [www.forticlient.com](http://www.forticlient.com).
2. Open the FortiClient Console and go to *Remote Access > Configure VPN*.
3. Add a new connection:
  - a. Set the connection name.
  - b. Set *Remote Gateway* to the IP of the listening FortiGate interface, in this example, *172.20.120.123*.
4. Select *Customize Port* and set it to *10443*.
5. Save your settings.
6. Log in using the *ldu1* credentials.

### To check the SSL VPN connection using the GUI:

1. Go to *VPN > Monitor > SSL-VPN Monitor* to verify the user's connection.
2. Go to *Log & Report > Events* and select *VPN Events* from the event type dropdown list to view the details of the SSL VPN connection event log.
3. Go to *Log & Report > Forward Traffic* to view the details of the SSL VPN traffic.

### To check the web portal login using the CLI:

```

get vpn ssl monitor
SSL VPN Login Users:
 Index User Auth Type Timeout From HTTP in/out HTTPS in/out
 0 ldu1 1(1) 229 10.1.100.254 0/0 0/0

```

```

SSL VPN sessions:
 Index User Source IP Duration I/O Bytes Tunnel/Dest IP

```

### To check the tunnel login using the CLI:

```

get vpn ssl monitor
SSL VPN Login Users:
 Index User Auth Type Timeout From HTTP in/out HTTPS in/out
 0 ldu1 1(1) 291 10.1.100.254 0/0 0/0

```

```

SSL VPN sessions:

```

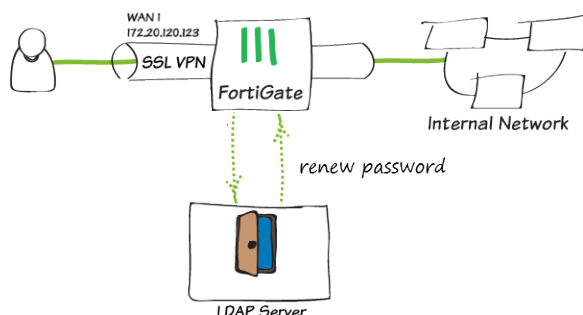
Index	User	Source IP	Duration	I/O Bytes	Tunnel/Dest IP
0	ldu1	10.1.100.254	9	22099/43228	10.212.134.200

## SSL VPN with LDAP user password renew

This is a sample configuration of SSL VPN for LDAP users with *Force Password Change on next logon*. In this example, the LDAP server is a Windows 2012 AD server. A user *ldu1* is configured on Windows 2012 AD server with *Force password change on next logon*.

You must have generated and exported a CA certificate from the AD server and then have imported it as an external CA certificate into the FortiGate.

### Sample topology



### Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface.

#### To configure SSL VPN using the GUI:

- Configure the interface and firewall address. The port1 interface connects to the internal network.
  - Go to *Network > Interfaces* and edit the *wan1* interface.
  - Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.
  - Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.
  - Click *OK*.
  - Go to *Policy & Objects > Address* and create an address for internet subnet *192.168.1.0*.
- Import CA certificate into FortiGate:
  - Go to *System > Features Visibility* and ensure *Certificates* is enabled.
  - Go to *System > Certificates* and select *Import > CA Certificate*.
  - Select *Local PC* and then select the certificate file.  
The CA certificate now appears in the list of *External CA Certificates*. In this example, it is called *CA\_Cert\_1*.
  - If you want, you can use CLI commands to rename the system-generated *CA\_Cert\_1* to be more descriptive:

```

config vpn certificate ca
 rename CA_Cert_1 to LDAPS-CA
end

```

### 3. Configure the LDAP user:



The LDAP user must either be an administrator, or have the proper permissions delegated to it, to be able to change passwords of other registered users on the LDAP server.

- a. Go to *User & Device > LDAP Servers > Create New*.
- b. Specify *Name* and *Server IP/Name*.
- c. Specify *Common Name Identifier* and *Distinguished Name*.
- d. Set *Bind Type* to *Regular*.
- e. Specify *Username* and *Password*.
- f. Enable *Secure Connection* and set *Protocol* to *LDAPS*.
- g. For *Certificate*, select *LDAP server CA LDAPS-CA* from the list.
- h. To enable the `password-renew` option, use these CLI commands:

```
config user ldap
 edit "ldaps-server"
 set password-expiry-warning enable
 set password-renewal enable
 next
end
```

### 4. Configure user group:

- a. Go to *User & Device > User Groups* to create a user group.
- b. Enter a *Name*.
- c. In *Remote Groups*, click *Add* to add *ldaps-server*.

### 5. Configure SSL VPN web portal:

- a. Go to *VPN > SSL-VPN Portals* to edit the *full-access* portal.  
This portal supports both web and tunnel mode.
- b. Disable *Enable Split Tunneling* so that all SSL VPN traffic goes through the FortiGate.

### 6. Configure SSL VPN settings:

- a. Go to *VPN > SSL-VPN Settings*.
- b. Select the *Listen on Interface(s)*, in this example, *wan1*.
- c. Set *Listen on Port* to *10443*.
- d. Set *Server Certificate* to the authentication certificate.
- e. Under *Authentication/Portal Mapping*, set default Portal *web-access* for *All Other Users/Groups*.
- f. Create new *Authentication/Portal Mapping* for group *ldaps-group* mapping portal *full-access*.

### 7. Configure SSL VPN firewall policy:

- a. Go to *Policy & Objects > IPv4 Policy*.
- b. Fill in the firewall policy name, in this example, *sslvpn certificate auth*.
- c. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.
- d. Set the *Source Address* to *all* and *Source User* to *ldaps-group*.
- e. Set the *Outgoing Interface* to the local network interface so that the remote user can access the internal network, in this example, *port1*.
- f. Set *Destination Address* to the internal protected subnet *192.168.1.0*.
- g. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.
- h. Enable *NAT*.

- i. Configure any remaining firewall and security options as desired.
- j. Click OK.

### To configure SSL VPN using the CLI:

#### 1. Configure the interface and firewall address.

```
config system interface
 edit "wan1"
 set vdom "root"
 set ip 172.20.120.123 255.255.255.0
 next
end
```

#### 2. Configure internal interface and protected subnet, then connect the port1 interface to the internal network.

```
config system interface
 edit "port1"
 set vdom "root"
 set ip 192.168.1.99 255.255.255.0
 next
end

config firewall address
 edit "192.168.1.0"
 set subnet 192.168.1.0 255.255.255.0
 next
end
```

#### 3. Import CA certificate into FortiGate.

- a. Go to *System > Features Visibility* and ensure *Certificates* is enabled.
- b. Go to *System > Certificates* and select *Import > CA Certificate*.
- c. Select *Local PC* and then select the certificate file.  
The CA certificate now appears in the list of *External CA Certificates*. In the example, it is called *CA\_Cert\_1*.
- d. If you want, you can use CLI commands to rename the system-generated *CA\_Cert\_1* to be more descriptive:

```
config vpn certificate ca
 rename CA_Cert_1 to LDAPS-CA
end
```

#### 4. Configure the LDAP server.



The LDAP user must either be an administrator, or have the proper permissions delegated to it, to be able to change passwords of other registered users on the LDAP server.

---

```
config user ldap
 edit "ldaps-server"
 set server "172.20.120.161"
 set cnid "cn"
 set dn "cn=Users,dc=qa,dc=fortinet,dc=com"
 set type regular
 set username "CN=Administrator,cn=users,DC=qa,DC=fortinet,DC=com"
 set password *****
 set group-member-check group-object
 set secure ldaps
```

```
 set ca-cert "LDAPS-CA"
 set port 636
 set password-expiry-warning enable
 set password-renewal enable
 next
end
```

#### 5. Configure user group.

```
config user group
 edit "ldaps-group"
 set member "ldaps-server"
 next
end
```

#### 6. Configure SSL VPN web portal.

```
config vpn ssl web portal
 edit "full-access"
 set tunnel-mode enable
 set web-mode enable
 set ip-pools "SSLVPN_TUNNEL_ADDR1"
 set split-tunneling disable
 next
end
```

#### 7. Configure SSL VPN settings.

```
config vpn ssl settings
 set servercert "server_certificate"
 set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
 set source-interface "wan1"
 set source-address "all"
 set default-portal "web-access"
 config authentication-rule
 edit 1
 set groups "ldaps-group"
 set portal "full-access"
 next
 end
end
```

#### 8. Configure one SSL VPN firewall policy to allow remote user to access the internal network.

```
config firewall policy
 edit 1
 set name "sslvpn web mode access"
 set srcintf "ssl.root"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "192.168.1.0"
 set groups "ldaps-group"
 set action accept
 set schedule "always"
 set service "ALL"
 set nat enable
 next
end
```

**To see the results of web portal:**

1. From a remote device, use a web browser to log into the SSL VPN web portal `http://172.20.120.123:10443`.
2. Log in using the `ldu1` credentials.  
Use a user that is configured on FortiAuthenticator with *Force password change on next login*.
3. Click *Login*. You are prompted to enter a new password. The prompt will timeout after 90 seconds.
4. Go to `VPN > Monitor > SSL-VPN Monitor` to verify the user's connection.

**To see the results of tunnel connection:**

1. Download FortiClient from [www.forticlient.com](http://www.forticlient.com).
2. Open the FortiClient Console and go to *Remote Access > Configure VPN*.
3. Add a new connection:
  - Set the connection name.
  - Set *Remote Gateway* to the IP of the listening FortiGate interface, in this example, `172.20.120.123`.
4. Select *Customize Port* and set it to `10443`.
5. Save your settings.
6. Log in using the `ldu1` credentials.  
You are prompted to enter a new password. The prompt will timeout after 90 seconds.

**To check the SSL VPN connection using the GUI:**

1. Go to `VPN > Monitor > SSL-VPN Monitor` to verify the user's connection.
2. Go to `Log & Report > Events` and select *VPN Events* from the event type dropdown list to view the details of the SSL VPN connection event log.
3. Go to `Log & Report > Forward Traffic` to view the details of the SSL VPN traffic.

**To check the web portal login using the CLI:**

```
get vpn ssl monitor
SSL VPN Login Users:
 Index User Auth Type Timeout From HTTP in/out HTTPS in/out
 0 ldu1 1(1) 229 10.1.100.254 0/0 0/0

SSL VPN sessions:
 Index User Source IP Duration I/O Bytes Tunnel/Dest IP
```

**To check the tunnel login using the CLI:**

```
get vpn ssl monitor
SSL VPN Login Users:
 Index User Auth Type Timeout From HTTP in/out HTTPS in/out
 0 ldu1 1(1) 291 10.1.100.254 0/0 0/0

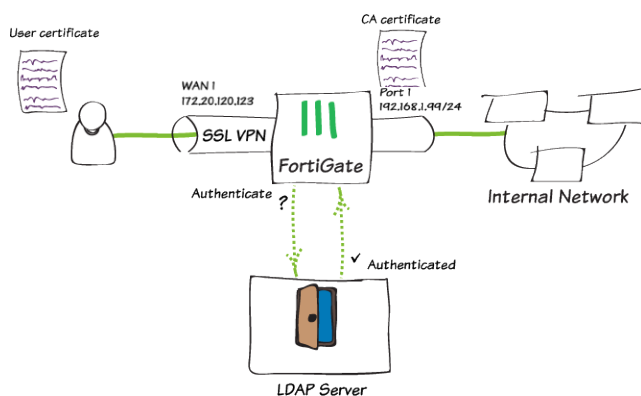
SSL VPN sessions:
 Index User Source IP Duration I/O Bytes Tunnel/Dest IP
 0 ldu1 10.1.100.254 9 22099/43228 10.212.134.200
```

## SSL VPN with LDAP-integrated certificate authentication

This is a sample configuration of SSL VPN that requires users to authenticate using a certificate with LDAP `UserPrincipalName` checking.

This sample uses Windows 2012R2 Active Directory acting as both the user certificate issuer, the certificate authority, and the LDAP server.

### Sample topology



### Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface.

In this sample, the *User Principal Name* is included in the subject name of the issued certificate. This is the user field we use to search LDAP in the connection attempt.

To use the user certificate, you must first install it on the user's PC. When the user tries to authenticate, the user certificate is checked against the CA certificate to verify that they match.

Every user should have a unique user certificate. This allows you to distinguish each user and revoke a specific user's certificate, such as if a user no longer has VPN access.

#### To install the server certificate:

The server certificate is used for authentication and for encrypting SSL VPN traffic.

1. Go to *System > Feature Visibility* and ensure *Certificates* is enabled.
2. Go to *System > Certificates* and select *Import > Local Certificate*.
  - Set *Type* to *Certificate*.
  - Choose the *Certificate file* and the *Key file* for your certificate, and enter the *Password*.
  - If desired, you can change the *Certificate Name*.

The server certificate now appears in the list of *Certificates*.

#### To install the CA certificate:

The CA certificate is the certificate that signed both the server certificate and the user certificate. In this example, it is used to authenticate SSL VPN users.

1. Go to *System > Certificates* and select *Import > CA Certificate*.
2. Select *Local PC* and then select the certificate file.  
The CA certificate now appears in the list of *External CA Certificates*. In this example, it is called *CA\_Cert\_1*.

### To configure SSL VPN using the GUI:

1. Configure the interface and firewall address. The port1 interface connects to the internal network.
  - a. Go to *Network > Interfaces* and edit the *wan1* interface.
  - b. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.
  - c. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.
  - d. Click OK.
  - e. Go to *Policy & Objects > Address* and create an address for internet subnet *192.168.1.0*.
2. Configure the LDAP server.
  - a. Go to *User & Device > LDAP Servers > Create New*.
    - Specify *Name* and *Server IP/Name*.
    - Set *Distinguished Name* to *dc=fortinet-fsso,dc=com*.
    - Set *Bind Type* to *Regular*.
    - Set *Username* to *cn=admin,ou=testing,dc=fortinet-fsso,dc=com*.
    - Set *Password*.

3. Configure PKI users and a user group.

To use certificate authentication, use the CLI to create PKI users.

```
config user peer
 edit user1
 set ca CA_Cert_1
 set ldap-server "ldap-AD"
 set ldap-mode principal-name
 next
end
```

When you have create a PKI user, a new menu is added to the GUI.

- a. Go to *User & Device > PKI* to see the new user.
  - b. Go to *User & Device > User > User Groups* and create a group *sslvpn-group*.
  - c. Add the PKI peer object you created as a local member of the group.
  - d. Add a remote group on the LDAP server and select the group of interest.  
You need these users to be members using the LDAP browser window.
4. Configure SSL VPN web portal.
  - a. Go to *VPN > SSL-VPN Portals* to edit the *full-access* portal.  
This portal supports both web and tunnel mode.
  - b. Disable *Enable Split Tunneling* so that all SSL VPN traffic goes through the FortiGate.
5. Configure SSL VPN settings.
  - a. Go to *VPN > SSL-VPN Settings*.
  - b. Select the *Listen on Interface(s)*, in this example, *wan1*.
  - c. Set *Listen on Port* to *10443*.
  - d. Set *Server Certificate* to the authentication certificate.
  - e. Enable *Require Client Certificate*.
  - f. Under *Authentication/Portal Mapping*, set default Portal *web-access* for *All Other Users/Groups*.
  - g. Create new *Authentication/Portal Mapping* for group *sslvpn-group* mapping portal *full-access*.



6. Configure SSL VPN firewall policy.
  - a. Go to *Policy & Objects > IPv4 Policy*.
  - b. Fill in the firewall policy name. In this example, *sslvpn certificate auth*.
  - c. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.
  - d. Set the *Source Address* to *all* and *Source User* to *sslvpn-group*.
  - e. Set the *Outgoing Interface* to the local network interface so that the remote user can access the internal network. In this example, *port1*.
  - f. Set *Destination Address* to the internal protected subnet *192.168.1.0*.
  - g. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.
  - h. Enable *NAT*.
  - i. Configure any remaining firewall and security options as desired.
  - j. Click *OK*.

### To configure SSL VPN using the CLI:

1. Configure the interface and firewall address.

```
config system interface
 edit "wan1"
 set vdom "root"
 set ip 172.20.120.123 255.255.255.0
 next
end
```

2. Configure internal interface and protected subnet, then connect the port1 interface to the internal network.

```
config system interface
 edit "port1"
 set vdom "root"
 set ip 192.168.1.99 255.255.255.0
 next
end

config firewall address
 edit "192.168.1.0"
 set subnet 192.168.1.0 255.255.255.0
 next
end
```

3. Configure the LDAP server.

```
config user ldap
 edit "ldap-AD"
 set server "172.18.60.206"
 set cnid "cn"
 set dn "dc=fortinet-fsso,dc=com"
 set type regular
 set username "cn=admin,ou=testing,dc=fortinet-fsso,dc=com"
 set password ldap-server-password
 next
end
```

4. Configure PKI users and a user group.

```
config user peer
 edit user1
```

```
 set ca CA_Cert_1
 set ldap-server "ldap-AD"
 set ldap-mode principal-name
 next
end

config user group
 edit "sslvpn-group"
 set member "ldap-AD" "user1"
 config match
 edit 1
 set server-name "ldap-AD"
 set group-name "CN=group3,OU=Testing,DC=Fortinet-FSSO,DC=COM"
 next
 end
 next
end
```

#### 5. Configure SSL VPN web portal.

```
config vpn ssl web portal
 edit "full-access"
 set tunnel-mode enable
 set web-mode enable
 set ip-pools "SSLVPN_TUNNEL_ADDR1"
 set split-tunneling disable
 next
end
```

#### 6. Configure SSL VPN settings.

```
config vpn ssl settings
 set servercert "server_certificate"
 set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
 set source-interface "wan1"
 set source-address "all"
 set default-portal "web-access"
 set reqclientcert enable
 config authentication-rule
 edit 1
 set groups "sslvpn-group"
 set portal "full-access"
 next
 end
end
```

#### 7. Configure one SSL VPN firewall policy to allow remote user to access the internal network.

```
config firewall policy
 edit 1
 set name "sslvpn web mode access"
 set srcintf "ssl.root"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "192.168.1.0"
 set groups "sslvpn-group"
 set action accept
 set schedule "always"
```

```

 set service "ALL"
 set nat enable
 next
end

```

### To see the results of tunnel connection:

1. Download FortiClient from [www.forticlient.com](http://www.forticlient.com).
  2. Open the FortiClient Console and go to *Remote Access > Configure VPN*.
  3. Add a new connection.
    - Set the connection name.
    - Set *Remote Gateway* to the IP of the listening FortiGate interface, in this example, *172.20.120.123*.
  4. Select *Customize Port* and set it to *10443*.
  5. Enable *Client Certificate* and select the authentication certificate.
  6. Save your settings.
- Connecting to the VPN only requires the user's certificate. It does not require username or password.

### To see the results of web portal:

1. In a web browser, log into the portal *http://172.20.120.123:10443*.  
A message requests a certificate for authentication.
2. Select the user certificate.  
You can connect to the SSL VPN web portal.

### To check the SSL VPN connection using the GUI:

1. Go to *VPN > Monitor > SSL-VPN Monitor* to verify the list of SSL users.
2. Go to *Log & Report > VPN Events* to view the details of the SSL VPN connection event log.
3. Go to *Log & Report > Forward Traffic* to view the details of the SSL VPN traffic.

### To check the SSL VPN connection using the CLI:

Below is a sample output of `diagnose debug application fnbamd -1` while the user connects. This is a shortened output sample of a few locations to show the important parts. This sample shows lookups to find the group memberships (three groups total) of the user and that the correct group being found results in a match.

```

[1148] fnbamd_ldap_recv-Response len: 16, svr: 172.18.60.206
[829] fnbamd_ldap_parse_response-Got one MESSAGE. ID:4, type:search-result
[864] fnbamd_ldap_parse_response-ret=0
[1386] __fnbamd_ldap_primary_grp_next-Auth accepted
[910] __ldap_rxtx-Change state to 'Done'
[843] __ldap_rxtx-state 23(Done)
[925] fnbamd_ldap_send-sending 7 bytes to 172.18.60.206
[937] fnbamd_ldap_send-Request is sent. ID 5
[753] __ldap_stop-svr 'ldap-AD'
[53] ldap_dn_list_del_all-Del CN=test3,OU=Testing,DC=Fortinet-FSSO,DC=COM
[399] ldap_copy_grp_list-copied CN=group3,OU=Testing,DC=Fortinet-FSSO,DC=COM
[399] ldap_copy_grp_list-copied CN=Domain Users,CN=Users,DC=Fortinet-FSSO,DC=COM
[2088] fnbamd_auth_cert_check-Matching group 'sslvpn-group'
[2007] __match_ldap_group-Matching server 'ldap-AD' - 'ldap-AD'
[2015] __match_ldap_group-Matching group 'CN=group3,OU=Testing,DC=Fortinet-FSSO,DC=COM' -
'CN=group3,OU=Testing,DC=Fortinet-FSSO,DC=COM'

```

```
[2091] fnbamd_auth_cert_check-Group 'sslvpn-group' matched
[2120] fnbamd_auth_cert_result-Result for ldap svr[0] 'ldap-AD' is SUCCESS
[2126] fnbamd_auth_cert_result-matched user 'test3', matched group 'sslvpn-group'
```

You can also use `diagnose firewall auth list` to validate that a firewall user entry exists for the SSL VPN user and is part of the right groups.

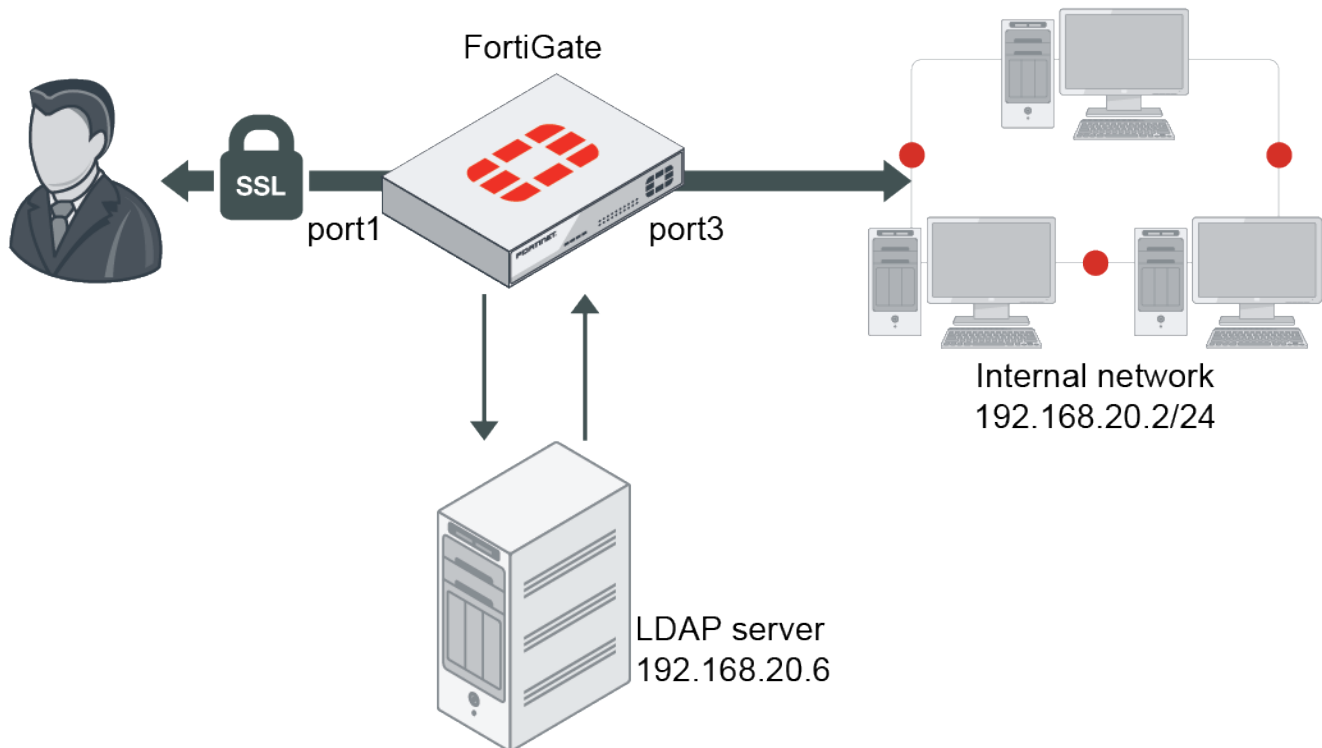
## SSL VPN for remote users with MFA and user case sensitivity

By default, remote LDAP and RADIUS user names are case sensitive. When a remote user object is applied to SSL VPN authentication, the user must type the exact case that is used in the user definition on the FortiGate.

Case sensitivity can be disabled by disabling the `username-sensitivity` CLI command, allowing the remote user object to match any case that the end user types in.

In this example, a remote user is configured with multi-factor authentication (MFA). The user group includes the LDAP user and server, and is applied to SSL VPN authentication and the policy.

### Topology



## Example configuration

### To configure the LDAP server:

1. Generate and export a CA certificate from the AD server .
2. Import the CA certificate into FortiGate:
  - a. Go to *System > Features Visibility* and ensure *Certificates* is enabled.
  - b. Go to *System > Certificates* and select *Import > CA Certificate*.
  - c. Select *Local PC* and then select the certificate file.  
The CA certificate now appears in the list of *External CA Certificates*. In this example, it is called *CA\_Cert\_1*.
  - d. If you want, you can use CLI commands to rename the system-generated *CA\_Cert\_1* to be more descriptive:

```
config vpn certificate ca
 rename CA_Cert_1 to LDAPS-CA
end
```

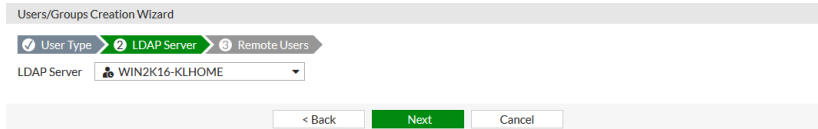
3. Configure the LDAP user:
  - a. Go to *User & Device > LDAP Servers* and click *Create New*.
  - b. Configure the following options for this example:

<b>Name</b>	WIN2K16-KLHOME
<b>Server IP/Name</b>	192.168.20.6
<b>Server Port</b>	636
<b>Common Name Identifier</b>	sAMAccountName
<b>Distinguished Name</b>	dc=KLHOME,dc=local
<b>Bind Type</b>	Regular
<b>Username</b>	KLHOME\Administrator
<b>Password</b>	*****
<b>Secure Connection</b>	Enable
<b>Protocol</b>	LDAPS
<b>Certificate</b>	CA_Cert_1 This is the CA certificate that you imported in step 2.

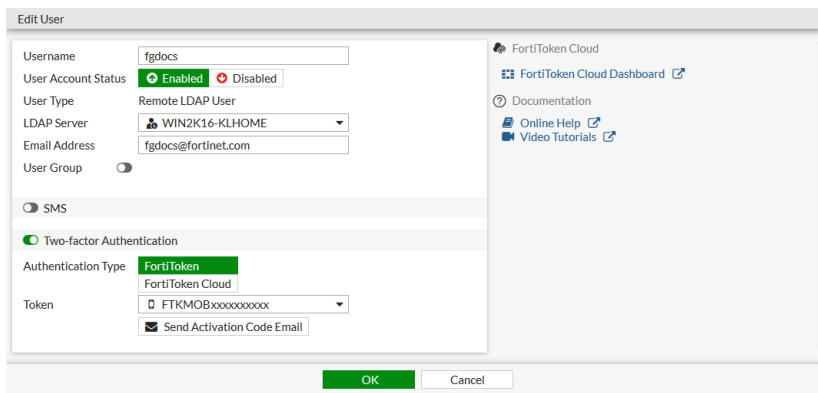
- c. Click *OK*.

### To configure an LDAP user with MFA:

1. Go to *User & Device > User Definition* and click *Create New*.
2. Select *Remote LDAP User*, then click *Next*.
3. Select the just created LDAP server, then click *Next*.



4. Right click to add the selected user, then click *Submit*.
5. Edit the user that you just created.  
The username will be pulled from the LDAP server with the same case as it has on the server.
6. Set the *Email Address* to the address that FortiGate will send the FortiToken to.
7. Enable *Two-factor Authentication*.
8. Set *Authentication Type* to *FortiToken*.
9. Set *Token* to a FortiToken device. See for more information.



10. Click *OK*.

### To disable case sensitivity on the remote user:

This can only be configured in the CLI.

```
config user local
 edit "fgdocs"
 set type ldap
 set two-factor fortitoken
 set fortitoken "FTKMOBxxxxxxxxx"
 set email-to "fgdocs@fortinet.com"
 set username-sensitivity disable
 set ldap-server "WIN2K16-KLHOME"
 next
end
```

### To configure a user group with the remote user and the LDAP server:

1. Go to *User & Device > User Groups* and click *Create New*.
2. Set the *Name* to *LDAP-USERGRP*.
3. Set *Members* to the just created remote user.

4. In the *Remote Groups* table, click *Add*:
  - a. Set *Remote Server* to the LDAP server.
  - b. Set the group or groups that apply, and right click to add them.
  - c. Click *OK*.

New User Group

Name: LDAP-USERGRP

Type: Firewall

Members: fgdocs

Remote Groups

Remote Server	Group Name
WIN2K16-KLHOME	

OK Cancel

5. Click *OK*.

#### To apply the user group to the SSL VPN portal:

1. Go to *VPN > SSL-VPN Settings*.
2. In the *Authentication/Portal Mapping* table, click *Create New*.
  - a. Set *Users/Groups* to the just created user group.
  - b. Configure the remaining settings as required.
  - c. Click *OK*.

SSL-VPN Settings

Authentication/Portal Mapping

Users/Groups	Realm	Portal
LDAP-USERGRP	/	tunnel-access
All Other Users/Groups	/	full-access

Apply

3. Click *Apply*.

#### To apply the user group to a firewall policy:

1. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
2. Configure the following:

<b>Name</b>	SSLVPNtoInternal
<b>Incoming Interface</b>	SSL-VPN tunnel interface (ssl.root)
<b>Outgoing Interface</b>	port3
<b>Source</b>	Address - SSLVPN_TUNNEL_ADDR1 User - LDAP-USERGRP
<b>Destination</b>	The address of the internal network.

	In this case: 192.168.20.0.
<b>Schedule</b>	always
<b>Service</b>	ALL
<b>Action</b>	ACCEPT
<b>NAT</b>	Enabled

3. Configuring the remaining settings as required.
4. Click OK.

### To configure this example in the CLI:

1. Configure the LDAP server:

```
config user ldap
 edit "WIN2K16-KLHOME"
 set server "192.168.20.6"
 set cnid "sAMAccountName"
 set dn "dc=KLHOME,dc=local"
 set type regular
 set username "KLHOME\\Administrator"
 set password *****
 set secure ldaps
 set ca-cert "CA_Cert_1"
 set port 636
 next
end
```

2. Configure an LDAP user with MFA and disable case and accent sensitivity on the remote user:

```
config user local
 edit "fgdocs"
 set type ldap
 set two-factor fortitoken
 set fortitoken "FTKMOBxxxxxxxxxx"
 set email-to "fgdocs@fortinet.com"
 set username-sensitivity disable
 end
```



```

 set ldap-server "WIN2K16-KLHOME"
 next
end

```

### 3. Configure a user group with the remote user and the LDAP server:

```

config user group
 edit "LDAP-USERGRP"
 set member "fgdocs" "WIN2K16-KLHOME"
 next
end

```

### 4. Apply the user group to the SSL VPN portal:

```

config vpn ssl settings
 set servercert <server certificate>
 set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
 set source-interface "port1"
 set source-address "all"
 set default-portal "web-access"
 config authentication-rule
 edit 1
 set groups "LDAP-USERGRP"
 set portal "full-access"
 next
 end
end

```

### 5. Apply the user group to a firewall policy:

```

config firewall policy
 edit 5
 set name "SSLVPNtoInternal"
 set srcintf "ssl.root"
 set dstintf "port3"
 set srcaddr "SSLVPN_TUNNEL_ADDR1"
 set dstaddr "192.168.20.0"
 set action accept
 set schedule "always"
 set service "ALL"
 set groups "LDAP-USERGRP"
 set nat enable
 next
end

```

## Verification

### To setup the VPN connection:

1. Download FortiClient from [www.forticlient.com](http://www.forticlient.com).
2. Open the FortiClient Console and go to *Remote Access*.
3. Add a new connection:
  - a. Set the connection name.
  - b. Set *Remote Gateway* to the IP of the listening FortiGate interface.
  - c. If required, set the *Customize Port*.
4. Save your settings.

**To test the connection with case sensitivity disabled:**

1. Connect to the VPN:
  - a. Log in to the tunnel with the username, using the same case that it is on the FortiGate.
  - b. When prompted, enter your FortiToken code.  
You should now be connected.

2. Check the web portal log in using the CLI:

```
get vpn ssl monitor
SSL VPN Login Users:
 Index User Group Auth Type Timeout From HTTP in/out HTTPS
in/out
 0 fgdocs LDAP-USERGRP 16(1) 289 192.168.2.202 0/0
0/0

SSL VPN sessions:
 Index User Group Source IP Duration I/O Bytes Tunnel/Dest IP
 0 fgdocs LDAP-USERGRP 192.168.2.202 45 99883/5572
10.212.134.200
```

3. Disconnect from the VPN connection.
4. Reconnect to the VPN:
  - a. Log in to the tunnel with the username, using a different case than on the FortiGate.
  - b. When prompted, enter your FortiToken code.  
You should now be connected.
5. Check the web portal log in using the CLI:

```
get vpn ssl monitor
SSL VPN Login Users:
 Index User Group Auth Type Timeout From HTTP in/out HTTPS
in/out
 0 FGDOCS LDAP-USERGRP 16(1) 289 192.168.2.202 0/0
0/0

SSL VPN sessions:
 Index User Group Source IP Duration I/O Bytes Tunnel/Dest IP
 0 FGDOCS LDAP-USERGRP 192.168.2.202 45 99883/5572
10.212.134.200
```

In both cases, the remote user is matched against the remote LDAP user object and prompted for multi-factor authentication.

**To test the connection with case sensitivity enabled:**

1. Enable case sensitivity for the user:

```
config user local
 edit "fgdocs"
 set username-sensitivity enable
 next
end
```

## 2. Connect to the VPN

- a. Log in to the tunnel with the username, using the same case that it is on the FortiGate.
- b. When prompted, enter your FortiToken code.  
You should now be connected.

## 3. Check the web portal log in using the CLI:

```
get vpn ssl monitor
SSL VPN Login Users:
 Index User Group Auth Type Timeout From HTTP in/out HTTPS
in/out
 0 fgdocs LDAP-USERGRP 16(1) 289 192.168.2.202 0/0
0/0

SSL VPN sessions:
 Index User Group Source IP Duration I/O Bytes Tunnel/Dest IP
0 fgdocs LDAP-USERGRP 192.168.2.202 45 99883/5572
10.212.134.200
```

## 1. Disconnect from the VPN connection.

## 2. Reconnect to the VPN:

- a. Log in to the tunnel with the username, using a different case than on the FortiGate.  
You will not be prompted for your FortiToken code. You should now be connected.

## 3. Check the web portal log in using the CLI:

```
get vpn ssl monitor
SSL VPN Login Users:
 Index User Group Auth Type Timeout From HTTP in/out HTTPS
in/out
 0 FGdocs LDAP-USERGRP 16(1) 289 192.168.2.202 0/0
0/0

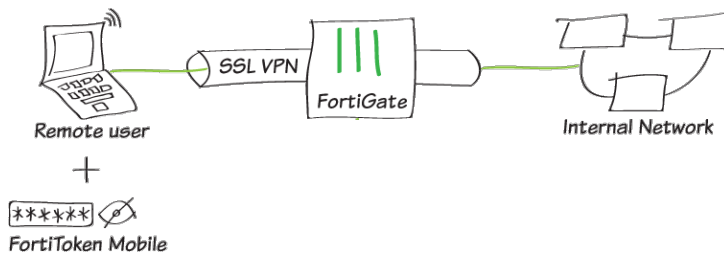
SSL VPN sessions:
 Index User Group Source IP Duration I/O Bytes Tunnel/Dest IP
0 FGdocs LDAP-USERGRP 192.168.2.202 45 99883/5572
10.212.134.200
```

In this case, the user is allowed to log in without a FortiToken code because the entered user name did not match the name defined on the remote LDAP user object. Authentication continues to be evaluated against the LDAP server though, which is not case sensitive.

## SSL VPN with FortiToken mobile push authentication

This is a sample configuration of SSL VPN that uses FortiToken mobile push two-factor authentication. If you enable push notifications, users can accept or deny the authentication request.

## Sample topology



## Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface.

### To configure SSL VPN using the GUI:

1. Configure the interface and firewall address. The port1 interface connects to the internal network.
  - a. Go to *Network > Interfaces* and edit the *wan1* interface.
  - b. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.
  - c. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.
  - d. Click **OK**.
  - e. Go to *Policy & Objects > Address* and create an address for internet subnet *192.168.1.0*.
2. Register FortiGate for FortiCare Support.  
To add or download a mobile token on FortiGate, FortiGate must be registered for FortiCare Support. If your FortiGate is registered, skip this step.
  - a. Go to *Dashboard > Licenses*.
  - b. Hover the pointer on *FortiCare Support* to check if FortiCare registered. If not, click it and select *Register*.
3. Add FortiToken mobile to FortiGate.  
If your FortiGate has FortiToken installed, skip this step.
  - a. Go to *User & Device > FortiTokens* and click *Create New*.
  - b. Select *Mobile Token* and type in *Activation Code*.
  - c. Every FortiGate has two free mobile tokens. Go to *User & Device > FortiTokens* and click *Import Free Trial Tokens*.
4. Enable FortiToken mobile push.  
To use FTM-push authentication, use CLI to enable FTM-Push on the FortiGate.
  - a. Ensure *server-ip* is reachable from the Internet and enter the following CLI commands:
 

```
config system ftm-push
 set server-ip 172.20.120.123
 set status enable
end
```
  - b. Go to *Network > Interfaces*.
  - c. Edit the *wan1* interface.
  - d. Under *Administrative Access > IPv4*, select *FTM*.
  - e. Click **OK**.

5. Configure user and user group.
  - a. Go to *User & Device > User Definition* to create a local user *sslvpnuser1*.
  - b. Enter the user's *Email Address*.
  - c. Enable *Two-factor Authentication* and select one mobile *Token* from the list.
  - d. Enable *Send Activation Code* and select *Email*.
  - e. Click *Next* and click *Submit*.
  - f. Go to *User & Device > User Groups* to create a group *sslvpngroup* with the member *sslvpnuser1*.
6. Activate the mobile token.
  - a. When the user *sslvpnuser1* is created, an email is sent to the user's email address. Follow the instructions to install your FortiToken mobile application on your device and activate your token.
7. Configure SSL VPN web portal.
  - a. Go to *VPN > SSL-VPN Portals* to edit the *full-access* portal.  
This portal supports both web and tunnel mode.
  - b. Disable *Enable Split Tunneling* so that all SSL VPN traffic goes through the FortiGate.
8. Configure SSL VPN settings.
  - a. Go to *VPN > SSL-VPN Settings*.
  - b. Select the *Listen on Interface(s)*, in this example, *wan1*.
  - c. Set *Listen on Port* to *10443*.
  - d. Set *Server Certificate* to the authentication certificate.
  - e. Under *Authentication/Portal Mapping*, set default Portal *web-access* for *All Other Users/Groups*.
  - f. Create new *Authentication/Portal Mapping* for group *sslvpngroup* mapping portal *full-access*.
9. Configure SSL VPN firewall policy.
  - a. Go to *Policy & Objects > IPv4 Policy*.
  - b. Fill in the firewall policy name. In this example, *sslvpn certificate auth*.
  - c. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.
  - d. Set the *Source Address* to *all* and *Source User* to *sslvpngroup*.
  - e. Set the *Outgoing Interface* to the local network interface so that the remote user can access the internal network. In this example, *port1*.
  - f. Set *Destination Address* to the internal protected subnet *192.168.1.0*.
  - g. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.
  - h. Enable *NAT*.
  - i. Configure any remaining firewall and security options as desired.
  - j. Click *OK*.

### To configure SSL VPN using the CLI:

1. Configure the interface and firewall address.

```
config system interface
 edit "wan1"
 set vdom "root"
 set ip 172.20.120.123 255.255.255.0
 next
end
```

2. Configure internal interface and protected subnet, then connect the port1 interface to the internal network.

```
config system interface
 edit "port1"
```

```
 set vdom "root"
 set ip 192.168.1.99 255.255.255.0
 next
end

config firewall address
 edit "192.168.1.0"
 set subnet 192.168.1.0 255.255.255.0
 next
end
```

### 3. Register FortiGate for FortiCare Support.

To add or download a mobile token on FortiGate, FortiGate must be registered for FortiCare Support. If your FortiGate is registered, skip this step.

```
diagnose forticare direct-registration product-registration -a "your account@xxx.com" -p
"your password" -T "Your Country/Region" -R "Your Reseller" -e 1
```

### 4. Add FortiToken mobile to FortiGate.

- a. If your FortiGate has FortiToken installed, skip this step.

```
execute fortitoken-mobile import <your FTM code>
```

- b. Every FortiGate has two free mobile Tokens. You can download the free token.

```
execute fortitoken-mobile import 0000-0000-0000-0000-0000
```

### 5. Enable FortiToken mobile push.

- a. To use FTM-push authentication, ensure `server-ip` is reachable from the Internet and enable FTM-push in the FortiGate.

```
config system ftm-push
 set server-ip 172.20.120.123
 set status enable
end
```

- b. Enable FTM service on WAN interface.

```
config system interface
 edit "wan1"
 append allowaccess ftm
 next
end
```

### 6. Configure user and user group.

```
config user local
 edit "sslvpnuser1"
 set type password
 set two-factor fortitoken
 set fortitoken <select mobile token for the option list>
 set email-to <user's email address>
 set passwd <user's password>
 next
end

config user group
 edit "sslvpngroup"
 set member "sslvpnuser1"
 next
end
```

**7. Activate the mobile token.**

- a. When the user *sslvpnuser1* is created, an email is sent to the user's email address. Follow the instructions to install your FortiToken mobile application on your device and activate your token.

**8. Configure SSL VPN web portal.**

```
config vpn ssl web portal
 edit "full-access"
 set tunnel-mode enable
 set web-mode enable
 set ip-pools "SSLVPN_TUNNEL_ADDR1"
 set split-tunneling disable
 next
end
```

**9. Configure SSL VPN settings.**

```
config vpn ssl settings
 set servercert "server_certificate"
 set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
 set source-interface "wan1"
 set source-address "all"
 set default-portal "web-access"
 config authentication-rule
 edit 1
 set groups "sslvpngroup"
 set portal "full-access"
 next
 end
end
```

**10. Configure one SSL VPN firewall policy to allow remote user to access the internal network.**

```
config firewall policy
 edit 1
 set name "sslvpn web mode access"
 set srcintf "ssl.root"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "192.168.1.0"
 set groups "sslvpngroup"
 set action accept
 set schedule "always"
 set service "ALL"
 set nat enable
 next
end
```

**To see the results of web portal:**

1. From a remote device, use a web browser to log into the SSL VPN web portal *http://172.20.120.123:10443*.
2. Log in using the *sslvpnuser1* credentials.  
The FortiGate pushes a login request notification through the FortiToken mobile application.
3. Check your mobile device and select *Approve*.  
When the authentication is approved, *sslvpnuser1* is logged into the SSL VPN portal.
4. On the FortiGate, go to *Monitor > SSL-VPN Monitor* to confirm the user connection.

**To see the results of tunnel connection:**

1. Download FortiClient from [www.forticlient.com](http://www.forticlient.com).
2. Open the FortiClient Console and go to *Remote Access > Configure VPN*.
3. Add a new connection.
  - Set the connection name.
  - Set *Remote Gateway* to the IP of the listening FortiGate interface, in this example, *172.20.120.123*.
4. Select *Customize Port* and set it to *10443*.
5. Save your settings.
6. Log in using the *sslvpnuser1* credentials and click *FTM Push*.  
The FortiGate pushes a login request notification through the FortiToken mobile application.
7. Check your mobile device and select *Approve*.  
When the authentication is approved, *sslvpnuser1* is logged into the SSL VPN tunnel.

**To check the SSL VPN connection using the GUI:**

1. Go to *VPN > Monitor > SSL-VPN Monitor* to verify the user's connection.
2. Go to *Log & Report > Forward Traffic* to view the details of the SSL VPN traffic.

**To check the web portal login using the CLI:**

```
get vpn ssl monitor
SSL VPN Login Users:
```

Index	User	Auth Type	Timeout	From	HTTP in/out	HTTPS in/out
0	sslvpnuser1	1 (1)	229	10.1.100.254	0/0	0/0

```
SSL VPN sessions:
```

Index	User	Source IP	Duration	I/O Bytes	Tunnel/Dest IP
-------	------	-----------	----------	-----------	----------------

**To check the tunnel login using the CLI:**

```
get vpn ssl monitor
SSL VPN Login Users:
```

Index	User	Auth Type	Timeout	From	HTTP in/out	HTTPS in/out
0	sslvpnuser1	1 (1)	291	10.1.100.254	0/0	0/0

```
SSL VPN sessions:
```

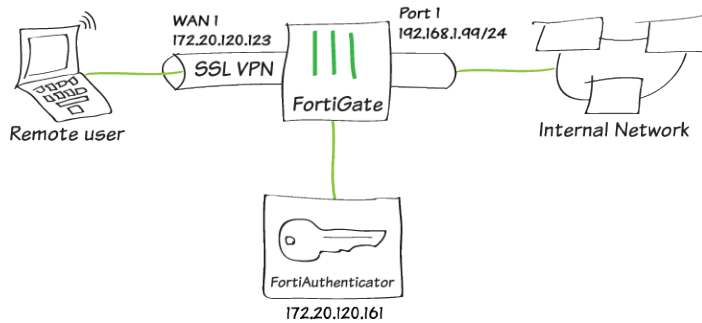
Index	User	Source IP	Duration	I/O Bytes	Tunnel/Dest IP
0	sslvpnuser1	10.1.100.254	9	22099/43228	10.212.134.200

**SSL VPN with RADIUS on FortiAuthenticator**

This is a sample configuration of SSL VPN that uses FortiAuthenticator as a RADIUS authentication server.



## Sample topology



## Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface.

### To configure FortiAuthenticator using the GUI:

1. Create a user on the FortiAuthenticator.
  - a. On the FortiAuthenticator, go to *Authentication > User Management > Local Users* to create a user *sslvpnuser1*.
  - b. Enable *Allow RADIUS authentication* and click *OK* to access additional settings.
  - c. Go to *Authentication > User Management > User Groups* to create a group *sslvpngroup*.
  - d. Add *sslvpnuser1* to the group by moving the user from *Available users* to *Selected users*.
2. Create the RADIUS client (FortiGate) on the FortiAuthenticator.
  - a. On the FortiAuthenticator, go to *Authentication > RADIUS Service > Clients* to add the FortiGate as a RADIUS client (*OfficeServer*).
  - b. Enter the FortiGate IP address and set a *Secret*.  
The secret is a pre-shared secure password that the FortiGate uses to authenticate to the FortiAuthenticator.
  - c. Set *Realms* to *local | Local users*.

### To configure SSL VPN using the GUI:

1. Configure the interface and firewall address. The port1 interface connects to the internal network.
  - a. Go to *Network > Interfaces* and edit the *wan1* interface.
  - b. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.
  - c. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.
  - d. Click *OK*.
  - e. Go to *Policy & Objects > Address* and create an address for internet subnet *192.168.1.0*.
2. Create a RADIUS user and user group .
  - a. On the FortiGate, go to *User & Device > RADIUS Servers* to create a user to connect to the RADIUS server (FortiAuthenticator).
  - b. For *Name*, use *FAC-RADIUS*.
  - c. Enter the IP address of the FortiAuthenticator, and enter the *Secret* created above.
  - d. Click *Test Connectivity* to ensure you can connect to the RADIUS server.
  - e. Select *Test User Credentials* and enter the credentials for *sslvpnuser1*.  
The FortiGate can now connect to the FortiAuthenticator as the RADIUS client.

- f. Go to *User & Device > User Groups* and click *Create New* to map authenticated remote users to a user group on the FortiGate.
  - g. For *Name*, use *SSLVPNGroup*.
  - h. In *Remote Groups*, click *Add*.
  - i. In the *Remote Server* dropdown list, select *FAC-RADIUS*.
  - j. Leave the *Groups* field blank.
3. Configure SSL VPN web portal.
  - a. Go to *VPN > SSL-VPN Portals* to edit the *full-access* portal.  
This portal supports both web and tunnel mode.
  - b. Disable *Enable Split Tunneling* so that all SSL VPN traffic goes through the FortiGate.
4. Configure SSL VPN settings.
  - a. Go to *VPN > SSL-VPN Settings*.
  - b. Select the *Listen on Interface(s)*, in this example, *wan1*.
  - c. Set *Listen on Port* to *10443*.
  - d. Set *Server Certificate* to the authentication certificate.
  - e. Under *Authentication/Portal Mapping*, set default Portal *web-access* for *All Other Users/Groups*.
  - f. Create new *Authentication/Portal Mapping* for group *sslvpngroup* mapping portal *full-access*.
5. Configure SSL VPN firewall policy.
  - a. Go to *Policy & Objects > IPv4 Policy*.
  - b. Fill in the firewall policy name. In this example, *sslvpn certificate auth*.
  - c. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.
  - d. Set the *Source Address* to *all* and *Source User* to *sslvpngroup*.
  - e. Set the *Outgoing Interface* to the local network interface so that the remote user can access the internal network. In this example: *port1*.
  - f. Set *Destination Address* to the internal protected subnet *192.168.1.0*.
  - g. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.
  - h. Enable *NAT*.
  - i. Configure any remaining firewall and security options as desired.
  - j. Click *OK*.

### To configure SSL VPN using the CLI:

1. Configure the interface and firewall address.

```
config system interface
 edit "wan1"
 set vdom "root"
 set ip 172.20.120.123 255.255.255.0
 next
end
```

2. Configure internal interface and protected subnet, then connect the port1 interface to the internal network.

```
config system interface
 edit "port1"
 set vdom "root"
 set ip 192.168.1.99 255.255.255.0
 next
end
```

```
config firewall address
 edit "192.168.1.0"
 set subnet 192.168.1.0 255.255.255.0
 next
end
```

### 3. Create a RADIUS user and user group.

```
config user radius
 edit "FAC-RADIUS"
 set server "172.20.120.161"
 set secret <FAC client secret>
 next
end

config user group
 edit "sslvpngroup"
 set member "FAC-RADIUS"
 next
end
```

### 4. Configure SSL VPN web portal.

```
config vpn ssl web portal
 edit "full-access"
 set tunnel-mode enable
 set web-mode enable
 set ip-pools "SSLVPN_TUNNEL_ADDR1"
 set split-tunneling disable
 next
end
```

### 5. Configure SSL VPN settings.

```
config vpn ssl settings
 set servercert "server_certificate"
 set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
 set source-interface "wan1"
 set source-address "all"
 set default-portal "web-access"
 config authentication-rule
 edit 1
 set groups "sslvpngroup"
 set portal "full-access"
 next
 end
end
```

### 6. Configure one SSL VPN firewall policy to allow remote user to access the internal network.

```
config firewall policy
 edit 1
 set name "sslvpn web mode access"
 set srcintf "ssl.root"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "192.168.1.0"
 set groups "sslvpngroup"
 set action accept
```

```

 set schedule "always"
 set service "ALL"
 set nat enable
 next
end

```

### To see the results of web portal:

1. From a remote device, use a web browser to log into the SSL VPN web portal <http://172.20.120.123:10443>.
2. Log in using the `sslvpnuser1` credentials.
3. On the FortiGate, go to *Monitor > SSL-VPN Monitor* to confirm the user connection.

### To see the results of tunnel connection:

1. Download FortiClient from [www.forticlient.com](http://www.forticlient.com).
2. Open the FortiClient Console and go to *Remote Access > Configure VPN*.
3. Add a new connection.
  - Set the connection name.
  - Set *Remote Gateway* to `172.20.120.123`.
4. Select *Customize Port* and set it to `10443`.
5. Save your settings.
6. Log in using the `sslvpnuser1` credentials and check that you are logged into the SSL VPN tunnel.

### To check the SSL VPN connection using the GUI:

1. Go to *VPN > Monitor > SSL-VPN Monitor* to verify the user's connection.
2. Go to *Log & Report > Forward Traffic* to view the details of the SSL VPN traffic.

### To check the web portal login using the CLI:

```

get vpn ssl monitor
SSL VPN Login Users:
 Index User Auth Type Timeout From HTTP in/out HTTPS in/out
 0 sslvpnuser1 1(1) 229 10.1.100.254 0/0 0/0

SSL VPN sessions:
 Index User Source IP Duration I/O Bytes Tunnel/Dest IP

```

### To check the tunnel login using the CLI:

```

get vpn ssl monitor
SSL VPN Login Users:
 Index User Auth Type Timeout From HTTP in/out HTTPS in/out
 0 sslvpnuser1 1(1) 291 10.1.100.254 0/0 0/0

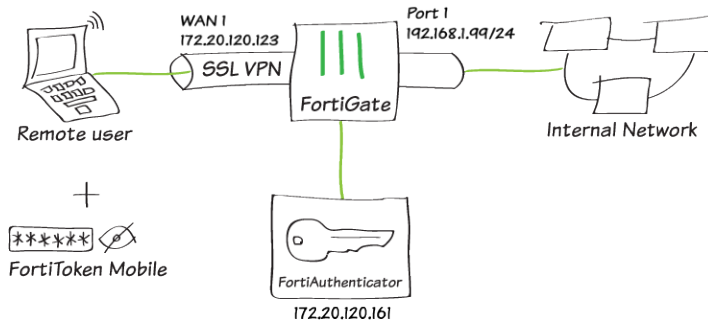
SSL VPN sessions:
 Index User Source IP Duration I/O Bytes Tunnel/Dest IP
 0 sslvpnuser1 10.1.100.254 9 22099/43228 10.212.134.200

```

## SSL VPN with RADIUS and FortiToken mobile push on FortiAuthenticator

This is a sample configuration of SSL VPN that uses FortiAuthenticator as a RADIUS authentication server and FortiToken mobile push two-factor authentication. If you enable push notifications, users can accept or deny the authentication request.

### Sample topology



### Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface.

#### To configure FortiAuthenticator using the GUI:

1. Add a FortiToken mobile license on the FortiAuthenticator.
  - a. On the FortiAuthenticator, go to *Authentication > User Management > FortiTokens*.
  - b. Click *Create New*.
  - c. Set *Token type* to *FortiToken Mobile* and enter the *FortiToken Activation codes*.
2. Create the RADIUS client (FortiGate) on the FortiAuthenticator.
  - a. On the FortiAuthenticator, go to *Authentication > RADIUS Service > Clients* to add the FortiGate as a RADIUS client (*OfficeServer*).
  - b. Enter the FortiGate IP address and set a *Secret*.  
The secret is a pre-shared secure password that the FortiGate uses to authenticate to the FortiAuthenticator.
  - c. Set *Authentication method* to *Enforce two-factor authentication*.
  - d. Select *Enable FortiToken Mobile push notifications authentication*.
  - e. Set *Realms* to *local | Local users*.
3. Create a user and assign FortiToken mobile to the user on the FortiAuthenticator.
  - a. On the FortiAuthenticator, go to *Authentication > User Management > Local Users* to create a user *sslvpnuser1*.
  - b. Enable *Allow RADIUS authentication* and click *OK* to access additional settings.
  - c. Enable *Token-based authentication* and select to deliver the token code by *FortiToken*.
  - d. Select the FortiToken added from the FortiToken Mobile dropdown menu.
  - e. Set *Delivery method* to *Email* and fill in the *User Information* section.
  - f. Go to *Authentication > User Management > User Groups* to create a group *sslvpngroup*.
  - g. Add *sslvpnuser1* to the group by moving the user from *Available users* to *Selected users*.

4. Install the FortiToken mobile application on your Android or iOS smartphone.  
The FortiAuthenticator sends the FortiToken mobile activation to the user's email address.
5. Activate the FortiToken mobile through the FortiToken mobile application by entering the activation code or scanning the QR code.

### To configure SSL VPN using the GUI:

1. Configure the interface and firewall address. The port1 interface connects to the internal network.
  - a. Go to *Network > Interfaces* and edit the *wan1* interface.
  - b. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.
  - c. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.
  - d. Click OK.
  - e. Go to *Policy & Objects > Address* and create an address for internet subnet *192.168.1.0*.
2. Create a RADIUS user and user group.
  - a. On the FortiGate, go to *User & Device > RADIUS Servers* to create a user to connect to the RADIUS server (FortiAuthenticator).
  - b. For *Name*, use *FAC-RADIUS*.
  - c. Enter the IP address of the FortiAuthenticator, and enter the *Secret* created above.
  - d. Click *Test Connectivity* to ensure you can connect to the RADIUS server.
  - e. Select *Test User Credentials* and enter the credentials for *sslvpnuser1*.  
The FortiGate can now connect to the FortiAuthenticator as the RADIUS client.
  - f. Go to *User & Device > User Groups* and click *Create New* to map authenticated remote users to a user group on the FortiGate.
  - g. For *Name*, use *SSLVPNGroup*.
  - h. In *Remote Groups*, click *Add*.
  - i. In the *Remote Server* dropdown list, select *FAC-RADIUS*.
  - j. Leave the *Groups* field blank.
3. Configure SSL VPN web portal.
  - a. Go to *VPN > SSL-VPN Portals* to edit the *full-access* portal.  
This portal supports both web and tunnel mode.
  - b. Disable *Enable Split Tunneling* so that all SSL VPN traffic goes through the FortiGate.
4. Configure SSL VPN settings.
  - a. Go to *VPN > SSL-VPN Settings*.
  - b. Select the *Listen on Interface(s)*, in this example, *wan1*.
  - c. Set *Listen on Port* to *10443*.
  - d. Set *Server Certificate* to the authentication certificate.
  - e. Under *Authentication/Portal Mapping*, set default Portal *web-access* for *All Other Users/Groups*.
  - f. Create new *Authentication/Portal Mapping* for group *sslvpngroup* mapping portal *full-access*.
5. Configure SSL VPN firewall policy.
  - a. Go to *Policy & Objects > IPv4 Policy*.
  - b. Fill in the firewall policy name. In this example, *sslvpn certificate auth*.
  - c. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.
  - d. Set the *Source Address* to *all* and *Source User* to *sslvpngroup*.
  - e. Set the *Outgoing Interface* to the local network interface so that the remote user can access the internal network. In this example: *port1*.
  - f. Set *Destination Address* to the internal protected subnet *192.168.1.0*.

- g. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.
- h. Enable *NAT*.
- i. Configure any remaining firewall and security options as desired.
- j. Click *OK*.

### To configure SSL VPN using the CLI:

#### 1. Configure the interface and firewall address.

```
config system interface
 edit "wan1"
 set vdom "root"
 set ip 172.20.120.123 255.255.255.0
 next
end
```

#### 2. Configure internal interface and protected subnet, then connect the port1 interface to the internal network.

```
config system interface
 edit "port1"
 set vdom "root"
 set ip 192.168.1.99 255.255.255.0
 next
end

config firewall address
 edit "192.168.1.0"
 set subnet 192.168.1.0 255.255.255.0
 next
end
```

#### 3. Create a RADIUS user and user group.

```
config user radius
 edit "FAC-RADIUS"
 set server "172.20.120.161"
 set secret <FAC client secret>
 next
end

config user group
 edit "sslvpngroup"
 set member "FAC-RADIUS"
 next
end
```

#### 4. Configure SSL VPN web portal.

```
config vpn ssl web portal
 edit "full-access"
 set tunnel-mode enable
 set web-mode enable
 set ip-pools "SSLVPN_TUNNEL_ADDR1"
 set split-tunneling disable
 next
end
```

## 5. Configure SSL VPN settings.

```
config vpn ssl settings
 set servercert "server_certificate"
 set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
 set source-interface "wan1"
 set source-address "all"
 set default-portal "web-access"
 config authentication-rule
 edit 1
 set groups "sslvpngroup"
 set portal "full-access"
 next
 end
end
```

## 6. Configure one SSL VPN firewall policy to allow remote user to access the internal network.

```
config firewall policy
 edit 1
 set name "sslvpn web mode access"
 set srcintf "ssl.root"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "192.168.1.0"
 set groups "sslvpngroup"
 set action accept
 set schedule "always"
 set service "ALL"
 set nat enable
 next
end
```

### To see the results of web portal:

1. From a remote device, use a web browser to log into the SSL VPN web portal <http://172.20.120.123:10443>.
2. Log in using the *sslvpnuser1* credentials.  
The FortiAuthenticator pushes a login request notification through the FortiToken Mobile application.
3. Check your mobile device and select *Approve*.  
When the authentication is approved, *sslvpnuser1* is logged into the SSL VPN portal.
4. On the FortiGate, go to *Monitor > SSL-VPN Monitor* to confirm the user connection.

### To see the results of tunnel connection:

1. Download FortiClient from [www.forticlient.com](http://www.forticlient.com).
2. Open the FortiClient Console and go to *Remote Access > Configure VPN*.
3. Add a new connection.
  - Set the connection name.
  - Set *Remote Gateway* to the IP of the listening FortiGate interface, in this example: *172.20.120.123*.
4. Select *Customize Port* and set it to *10443*.
5. Save your settings.
6. Log in using the *sslvpnuser1* credentials and click *FTM Push*.  
The FortiAuthenticator pushes a login request notification through the FortiToken Mobile application.



## 7. Check your mobile device and select *Approve*.

When the authentication is approved, *sslvpnuser1* is logged into the SSL VPN tunnel.

### To check the SSL VPN connection using the GUI:

1. Go to *VPN > Monitor > SSL-VPN Monitor* to verify the user's connection.
2. Go to *Log & Report > Forward Traffic* to view the details of the SSL VPN traffic.

### To check the web portal login using the CLI:

```
get vpn ssl monitor
```

SSL VPN Login Users:

Index	User	Auth Type	Timeout	From	HTTP in/out	HTTPS in/out
0	sslvpnuser1	1 (1)	229	10.1.100.254	0/0	0/0

SSL VPN sessions:

Index	User	Source IP	Duration	I/O Bytes	Tunnel/Dest IP
-------	------	-----------	----------	-----------	----------------

### To check the tunnel login on CLI:

```
get vpn ssl monitor
```

SSL VPN Login Users:

Index	User	Auth Type	Timeout	From	HTTP in/out	HTTPS in/out
0	sslvpnuser1	1 (1)	291	10.1.100.254	0/0	0/0

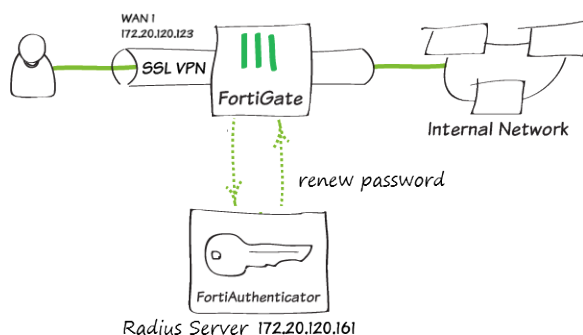
SSL VPN sessions:

Index	User	Source IP	Duration	I/O Bytes	Tunnel/Dest IP
0	sslvpnuser1	10.1.100.254	9	22099/43228	10.212.134.200

## SSL VPN with RADIUS password renew on FortiAuthenticator

This is a sample configuration of SSL VPN for RADIUS users with *Force Password Change on next logon*. In this example, the RADIUS server is a FortiAuthenticator. A user *test1* is configured on FortiAuthenticator with *Force password change on next logon*.

### Sample topology



## Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface.

### To configure SSL VPN using the GUI:

1. Configure the interface and firewall address. The port1 interface connects to the internal network.
  - a. Go to *Network > Interfaces* and edit the *wan1* interface.
  - b. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.
  - c. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.
  - d. Click *OK*.
  - e. Go to *Policy & Objects > Address* and create an address for internet subnet *192.168.1.0*.
2. Create a RADIUS user.
  - a. Go to *User & Device > RADIUS Servers* to create a user.
  - b. Set *Authentication method* to *MS-CHAP-v2*.
  - c. Enter the *IP/Name* and *Secret*.
  - d. Click *Create*.  
Password renewal only works with the MS-CHAP-v2 authentication method.
  - e. To enable the `password-renew` option, use these CLI commands.

```
config user radius
 edit "fac"
 set server "172.20.120.161"
 set secret <fac radius password>
 set auth-type ms_chap_v2
 set password-renewal enable
 next
end
```

3. Configure user group.
  - a. Go to *User & Device > User Groups* to create a user group.
  - b. For the *Name*, enter *fac-group*.
  - c. In *Remote Groups*, click *Add* to add *Remote Server* you just created.
4. Configure SSL VPN web portal.
  - a. Go to *VPN > SSL-VPN Portals* to edit the *full-access* portal.  
This portal supports both web and tunnel mode.
  - b. Disable *Enable Split Tunneling* so that all SSL VPN traffic goes through the FortiGate.
5. Configure SSL VPN settings.
  - a. Go to *VPN > SSL-VPN Settings*.
  - b. Select the *Listen on Interface(s)*, in this example, *wan1*.
  - c. Set *Listen on Port* to *10443*.
  - d. Set *Server Certificate* to the authentication certificate.
  - e. Under *Authentication/Portal Mapping*, set default Portal *web-access* for *All Other Users/Groups*.
  - f. Create new *Authentication/Portal Mapping* for group *fac-group* mapping portal *full-access*.
6. Configure SSL VPN firewall policy.
  - a. Go to *Policy & Objects > IPv4 Policy*.
  - b. Fill in the firewall policy name, in this example, *sslvpn certificate auth*.
  - c. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.

- d. Set the *Source Address* to *all* and *Source User* to *fac-group*.
- e. Set the *Outgoing Interface* to the local network interface so that the remote user can access the internal network, in this example, *port1*.
- f. Set *Destination Address* to the internal protected subnet *192.168.1.0*.
- g. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.
- h. Enable NAT.
- i. Configure any remaining firewall and security options as desired.
- j. Click OK.

### To configure SSL VPN using the CLI:

1. Configure the interface and firewall address.

```
config system interface
 edit "wan1"
 set vdom "root"
 set ip 172.20.120.123 255.255.255.0
 next
end
```

2. Configure internal interface and protected subnet, then connect the port1 interface to the internal network.

```
config system interface
 edit "port1"
 set vdom "root"
 set ip 192.168.1.99 255.255.255.0
 next
end

config firewall address
 edit "192.168.1.0"
 set subnet 192.168.1.0 255.255.255.0
 next
end
```

3. Configure the RADIUS server.

```
config user radius
 edit "fac"
 set server "172.18.58.107"
 set secret <fac radius password>
 set auth-type ms_chap_v2
 set password-renewal enable
 next
end
```

4. Configure user group.

```
config user group
 edit "fac-group"
 set member "fac"
 next
end
```

5. Configure SSL VPN web portal.

```
config vpn ssl web portal
 edit "full-access"
```

```
 set tunnel-mode enable
 set web-mode enable
 set ip-pools "SSLVPN_TUNNEL_ADDR1"
 set split-tunneling disable
 next
end
```

## 6. Configure SSL VPN settings.

```
config vpn ssl settings
 set servercert "server_certificate"
 set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
 set source-interface "wan1"
 set source-address "all"
 set default-portal "web-access"
 config authentication-rule
 edit 1
 set groups "fac-group"
 set portal "full-access"
 next
 end
end
```

## 7. Configure one SSL VPN firewall policy to allow remote user to access the internal network.

```
config firewall policy
 edit 1
 set name "sslvpn web mode access"
 set srcintf "ssl.root"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "192.168.1.0"
 set groups "fac-group"
 set action accept
 set schedule "always"
 set service "ALL"
 set nat enable
 next
end
```

### To see the results of web portal:

1. From a remote device, use a web browser to log into the SSL VPN web portal <http://172.20.120.123:10443>.
2. Log in using the *test1* credentials.  
Use a user which is configured on FortiAuthenticator with *Force password change on next login*.
3. Click *Login*. You are prompted to enter a new password.
4. Go to *VPN > Monitor > SSL-VPN Monitor* to verify the user's connection.

### To see the results of tunnel connection:

1. Download FortiClient from [www.forticlient.com](http://www.forticlient.com).
2. Open the FortiClient Console and go to *Remote Access > Configure VPN*.
3. Add a new connection.
  - Set the connection name.
  - Set *Remote Gateway* to the IP of the listening FortiGate interface, in this example, *172.20.120.123*.

4. Select *Customize Port* and set it to *10443*.
5. Save your settings.
6. Log in using the *test1* credentials.  
You are prompted to enter a new password.

#### To check the SSL VPN connection using the GUI:

1. Go to *VPN > Monitor > SSL-VPN Monitor* to verify the user's connection.
2. Go to *Log & Report > Events* and select *VPN Events* from the event type dropdown list to view the details of the SSL VPN connection event log.
3. Go to *Log & Report > Forward Traffic* to view the details of the SSL VPN traffic.

#### To check the web portal login using the CLI:

```
get vpn ssl monitor
SSL VPN Login Users:
```

Index	User	Auth Type	Timeout	From	HTTP in/out	HTTPS in/out
0	test1	1(1)	229	10.1.100.254	0/0	0/0

```
SSL VPN sessions:
```

Index	User	Source IP	Duration	I/O Bytes	Tunnel/Dest IP
-------	------	-----------	----------	-----------	----------------

#### To check the tunnel login using the CLI:

```
get vpn ssl monitor
SSL VPN Login Users:
```

Index	User	Auth Type	Timeout	From	HTTP in/out	HTTPS in/out
0	test1	1(1)	291	10.1.100.254	0/0	0/0

```
SSL VPN sessions:
```

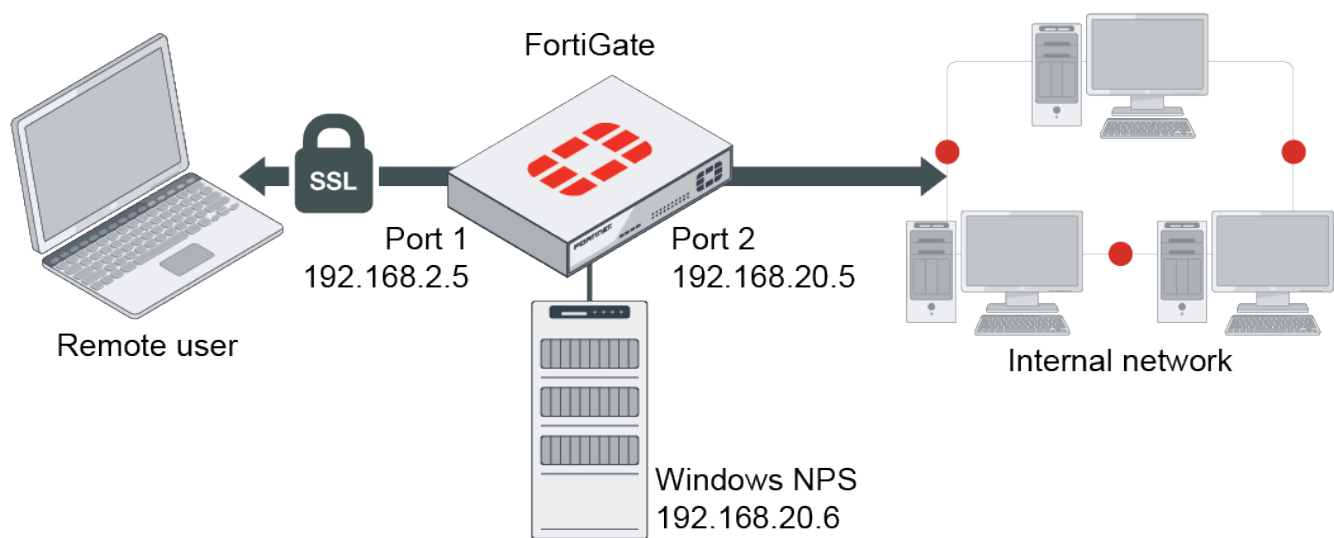
Index	User	Source IP	Duration	I/O Bytes	Tunnel/Dest IP
0	test1	10.1.100.254	9	22099/43228	10.212.134.200

## SSL VPN with RADIUS on Windows NPS

This is an example configuration of SSL VPN that uses Windows Network Policy Server (NPS) as a RADIUS authentication server.

The NPS must already be configured to accept the FortiGate as a RADIUS client and the choice of authentication method, such as MS-CHAPv2. A shared key must also have been created.

## Example



The user is connecting from their PC to the FortiGate's port1 interface. RADIUS authentication occurs between the FortiGate and the Windows NPS, and the SSL-VPN connection is established once the authentication is successful.

## Configure SSL-VPN with RADIUS on Windows NPS in the GUI

### To configure the internal and external interfaces:

1. Go to *Network > Interfaces*
2. Edit the *port1* interface and set *IP/Network Mask* to *192.168.2.5/24*.
3. Edit the *port2* interface and set *IP/Network Mask* to *192.168.20.5/24*.
4. Click *OK*.

### To create a firewall address:

1. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
2. Set *Name* to *192.168.20.0*.
3. Leave *Type* as *Subnet*
4. Set *Subnet / IP Range* to *192.168.20.0*.
5. Click *OK*.

### To add the RADIUS server:

1. Go to *User & Device > RADIUS Servers* and click *Create New*.
2. Set *Name* to *rad-server*.
3. Leave *Authentication method* set to *Default*. The PAP, MS-CHAPv2, and CHAP methods will be tried in order.
4. Under *Primary Server*, set *IP/Name* to *192.168.20.6* and *Secret* to the shared secret configured on the RADIUS server.
5. Click *Test Connectivity* to test the connection to the server, and ensure that *Connection status* is *Successful*.

6. Optionally, click *Test User Credentials* to test user credentials. Testing from the GUI is limited to PAP.

7. Click **OK**.

### To configure a user group:

1. Go to *User & Device > User Groups* and click *Create New*.
2. Set *Name* to *rad-group*.
3. Under *Remote Groups*, click *Add* and add the *rad-server*.

Remote Server	Group Name
rad-server	Any

4. Click **OK**.

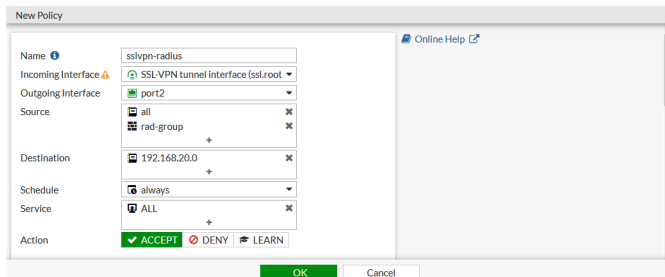
### To configure SSL VPN settings:

1. Go to *VPN > SSL-VPN Settings*.
2. Select the *Listen on Interface(s)*, in this example, *port1*.
3. Set *Listen on Port* to *10443*.
4. If you have a server certificate, set *Server Certificate* to the authentication certificate.
5. Under *Authentication/Portal Mapping*:
  - a. Edit *All Other Users/Groups* and set *Portal* to *web-access*.
  - b. Click *Create New* and create a mapping for the *rad-group* user group with *Portal* set to *full-access*.

- c. Click **OK**.
6. Configure other settings as required.
  7. Click **Apply**.

### To configure an SSL VPN firewall policy:

1. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
2. Set the policy name, in this example, *sslvpn-radius*.
3. Set *Incoming Interface* to *SSL-VPN tunnel interface(ssl.root)*.
4. Set *Outgoing Interface* to the local network interface so that the remote user can access the internal network. In this example, *port2*.
5. Set the *Source > Address* to *all* and *Source > User* to *rad-group*.
6. Set *Destination > Address* to the internal protected subnet *192.168.20.0*.
7. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.
8. Enable *NAT*.



9. Configure the remaining options as required.
10. Click **OK**.

### Configure SSL-VPN with RADIUS on Windows NPS in the CLI

#### To configure SSL VPN using the CLI:

1. Configure the internal and external interfaces:

```
config system interface
 edit "port1"
 set vdom "root"
 set ip 192.168.2.5 255.255.255.0
 set alias internal
 next
 edit "port2"
 set vdom "root"
 set ip 192.168.20.5 255.255.255.0
 set alias external
 next
end
```

2. Configure the firewall address:

```
config firewall address
 edit "192.168.20.0"
 set subnet 192.168.20.0 255.255.255.0
 next
end
```

3. Add the RADIUS server:

```
config user radius
 edit "rad-server"
```



```
 set server "192.168.20.6"
 set secret *****
 next
end
```

**4. Create a user group and add the RADIUS server to it:**

```
config user group
 edit "rad-group"
 set member "rad-server"
 next
end
```

**5. Configure SSL VPN settings:**

```
config vpn ssl settings
 set servercert "server_certificate"
 set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
 set source-interface "port1"
 set source-address "all"
 set default-portal "web-access"
 config authentication-rule
 edit 1
 set groups "rad-group"
 set portal "full-access"
 next
 end
end
```

**6. Configure an SSL VPN firewall policy to allow remote user to access the internal network.**

```
config firewall policy
 edit 1
 set name "sslvpn-radius"
 set srcintf "ssl.root"
 set dstintf "port2"
 set srcaddr "all"
 set dstaddr "192.168.20.0"
 set groups "rad-group"
 set action accept
 set schedule "always"
 set service "ALL"
 set nat enable
 next
end
```

## Results

### To connect with FortiClient in tunnel mode:

1. Download FortiClient from [www.forticlient.com](http://www.forticlient.com).
2. Open the FortiClient Console and go to *Remote Access > Configure VPN*.
3. Add a new connection:
  - a. Set the connection name.
  - b. Set *Remote Gateway* to *192.168.2.5*.
  - c. Select *Customize Port* and set it to *10443*.

4. Save your settings.
5. Log in using the RADIUS user credentials.

#### To check the SSL VPN connection using the GUI:

1. Go to *Monitor > SSL-VPN* to verify the user's connection.
2. Go to *Log & Report > Events* and select *VPN Events* from the event type drop-down list to view the details of the SSL VPN connection event log.
3. Go to *Log & Report > Forward Traffic* to view the details of the SSL VPN traffic.

#### To check the login using the CLI:

```
get vpn ssl monitor
```

```
SSL VPN Login Users:
```

Index	User	Group	Auth Type	Timeout	From	HTTP in/out	HTTPS in/out
0	radkeith		rad-group	2 (1)	295	192.168.2.202	0/0 0/0

```
SSL VPN sessions:
```

Index	User	Group	Source IP	Duration	I/O Bytes	Tunnel/Dest IP
0	radkeith		rad-group	192.168.2.202	18	28502/4966

10.212.134.200

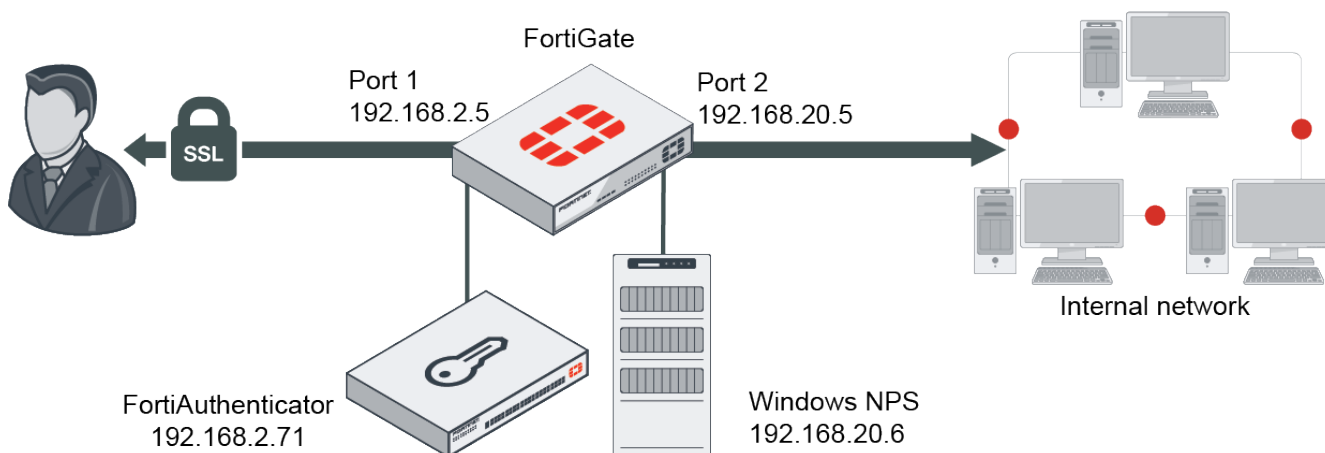
## SSL VPN with multiple RADIUS servers

When configuring two or more RADIUS servers, you can configure a Primary and Secondary server within the same RADIUS server configurations for backup purposes. You can also configure multiple RADIUS servers within the same User Group to service the access request at the same time.



A tertiary server can be configured in the CLI.

## Sample topology



## Sample configurations

- [Configure a Primary and Secondary server for backup on page 1437](#)
- [Authenticating to two RADIUS servers concurrently on page 1441](#)

### Configure a Primary and Secondary server for backup

When you define a Primary and Secondary RADIUS server, the access request will always be sent to the Primary server first. If the request is denied with an Access-Reject, then the user authentication fails. However, if there is no response from the Primary server after another attempt, the access request will be sent to the Secondary server.

In this example, you will use a Windows NPS server as the Primary server and a FortiAuthenticator as the Secondary server. It is assumed that users are synchronized between the two servers.

#### To configure the internal and external interfaces:

1. Go to *Network > Interfaces*.
2. Edit the *port1* interface and set *IP/Network Mask* to *192.168.2.5/24*.
3. Edit the *port2* interface and set *IP/Network Mask* to *192.168.20.5/24*.
4. Click *OK*.

#### To create a firewall address:

1. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
2. Set *Name* to *192.168.20.0*.
3. Leave *Type* as *Subnet*.
4. Set *IP/Netmask* to *192.168.20.0/24*.
5. Click *OK*.

#### To add the RADIUS server:

1. Go to *User & Device > RADIUS Servers* and click *Create New*.
2. Set *Name* to *PrimarySecondary*.
3. Leave *Authentication method* set to *Default*. The PAP, MS-CHAPv2, and CHAP methods will be tried in order.
4. Under *Primary Server*, set *IP/Name* to *192.168.20.6* and *Secret* to the shared secret configured on the RADIUS server.
5. Click *Test Connectivity* to test the connection to the server, and ensure that *Connection status* is *Successful*.
6. Under *Secondary Server*, set *IP/Name* to *192.168.2.71* and *Secret* to the shared secret configured on the RADIUS server.
7. Click *Test Connectivity* to test the connection to the server, and ensure that *Connection status* is *Successful*.
8. Click *OK*.

#### To configure the user group:

1. Go to *User & Authentication > User Groups* and click *Create New*.
2. In the *Name* field, enter *PrimarySecondaryGroup*.
3. In the *Remote Groups* area, click *Add*, and from the *Remote Server* dropdown, select *PrimarySecondary*.
4. Click *OK*, and then click *OK* again.

**To configure the SSL VPN settings:**

1. Go to *VPN > SSL-VPN Settings*.
2. From the *Listen on Interface(s)* dropdown select *port1*.
3. In the *Listen on Port* field enter *10443*.
4. Optionally, from the *Server Certificate* dropdown, select the authentication certificate if you have one for this SSL VPN portal.
5. Under *Authentication/Portal Mapping*, set the default portal web-access.
  - a. Select *All Other Users/Groups* and click *Edit*.
  - b. From the *Portal* dropdown, select *web-access*.
  - c. Click *OK*.
6. Create a web portal for *PrimarySecondaryGroup*.
  - a. Under *Authentication/Portal Mapping*, click *Create New*.
  - b. Click *Users/Groups* and select *PrimarySecondaryGroup*.
  - c. From the *Portal* dropdown, select *full-access*.
  - d. Click *OK*.

**To configure SSL VPN firewall policy:**

1. Go to *Policy & Objects > IPv4 Policy*.
2. Click *Create New* to create a new policy, or double-click an existing policy to edit it and configure settings.

<b>Name</b>	Enter the firewall policy name.
<b>Incoming Interface</b>	Select <i>SSL-VPN tunnel interface (ssl.root)</i> .
<b>Outgoing interface</b>	Set to the local network interface so that the remote user can access the internal network. For this example, select <i>port3</i> .
<b>Source</b>	In the <i>Address</i> tab select <i>SSLVPN_TUNNEL_ADDR1</i> . In the <i>User</i> tab, select <i>PrimarySecondaryGroup</i> .
<b>Destination</b>	Select the internal protected subnet <i>192.168.20.0</i> .
<b>Schedule</b>	Select <i>always</i> .
<b>Service</b>	Select <i>All</i> .
<b>Action</b>	Select <i>Accept</i> .
<b>NAT</b>	Set to <i>Enable</i> .

3. Configure any remaining firewall and security options as desired.
4. Click *OK*.

**To configure SSL VPN using the CLI:**

1. Configure the internal interface and firewall address.

```
config system interface
 edit "port3"
 set vdom "root"
 set ip 192.168.20.5 255.255.255.0
 set alias "internal"
 next
```

```
end
config firewall address
 edit "192.168.20.0"
 set uuid cc41eec2-9645-51ea-d481-5c5317f865d0
 set subnet 192.168.20.0 255.255.255.0
 next
end
```

## 2. Configure the RADIUS server.

```
config user radius
 edit "PrimarySecondary"
 set server "192.168.20.6"
 set secret <secret>
 set secondary-server "192.168.2.71"
 set secondary-secret <secret>
 next
end
```

## 3. Add the RADIUS user to the user group.

```
config user group
 edit "PrimarySecondaryGroup"
 set member "PrimarySecondary "
 next
end
```

## 4. Configure SSL VPN settings.

```
config vpn ssl settings
 set servercert "server_certificate"
 set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
 set source-interface "port1"
 set source-address "all"
 set default-portal "web-access"
 config authentication-rule
 edit 1
 set groups "PrimarySecondaryGroup "
 set portal "full-access"
 next
 end
end
```

## 5. Configure one SSL VPN firewall policy to allow remote users to access the internal network.

```
config firewall policy
 edit 1
 set name "sslvpn-radius"
 set srcintf "ssl.root"
 set dstintf "port3"
 set srcaddr "all"
 set dstaddr "192.168.20.0"
 set groups "PrimarySecondaryGroup"
 set action accept
 set schedule "always"
 set service "ALL"
 set nat enable
 next
end
```

### To verify the connection:

User *radkeith* is a member of both the NPS server and the FAC server.

When the Primary server is up, it will connect to the SSL VPN tunnel using FortiClient.

```
diag sniffer packet any 'port 1812' 4 0 1
interfaces=[any]
filters=[port 1812]
2020-05-15 16:26:50.838453 port3 out 192.168.20.5.2374 -> 192.168.20.6.1812: udp 118
2020-05-15 16:26:50.883166 port3 in 192.168.20.6.1812 -> 192.168.20.5.2374: udp 20
2020-05-15 16:26:50.883374 port3 out 192.168.20.5.2374 -> 192.168.20.6.1812: udp 182
2020-05-15 16:26:50.884683 port3 in 192.168.20.6.1812 -> 192.168.20.5.2374: udp 228
```

The access request is sent to the Primary NPS server 192.168.20.6, and the connection is successful.

```
get vpn ssl monitor
SSL VPN Login Users:
```

Index in/out	User HTTPS in/out	Group	Auth Type	Timeout	From	HTTP
0 0/0	radkeith 0/0	PrimarySecondaryGroup	2(1)	285	192.168.2.202	

SSL VPN sessions:

Index Tunnel/Dest IP	User	Group	Source IP	Duration	I/O Bytes
0 10.212.134.200	radkeith	PrimarySecondaryGroup	192.168.2.202	62	132477/4966

When the Primary server is down, and the Secondary server is up, the connection is made to the SSLVPN tunnel again:

```
diag sniffer packet any 'port 1812' 4 0 1
interfaces=[any]
filters=[port 1812]
2020-05-15 16:31:23.016875 port3 out 192.168.20.5.7989 -> 192.168.20.6.1812: udp 118
2020-05-15 16:31:28.019470 port3 out 192.168.20.5.7989 -> 192.168.20.6.1812: udp 118
2020-05-15 16:31:30.011874 port1 out 192.168.2.5.23848 -> 192.168.2.71.1812: udp 118
2020-05-15 16:31:30.087564 port1 in 192.168.2.71.1812 -> 192.168.2.5.23848: udp 20
```

Access request is sent to the Primary NPS server 192.168.20.6, but there was no response. RADIUS authentication falls through to the Secondary FortiAuthenticator 192.168.2.71, and the authentication was accepted. The VPN connection is established.

```
get vpn ssl monitor
SSL VPN Login Users:
```

Index in/out	User HTTPS in/out	Group	Auth Type	Timeout	From	HTTP
0 0/0	radkeith 0/0	PrimarySecondaryGroup	2(1)	287	192.168.2.202	

SSL VPN sessions:

Index Tunnel/Dest IP	User	Group	Source IP	Duration	I/O Bytes
0 10.212.134.200	radkeith	PrimarySecondaryGroup	192.168.2.202	48	53544/4966

## Authenticating to two RADIUS servers concurrently

There are times where users are located on separate RADIUS servers. This may be the case when migrating from an old server to a new one for example. In this scenario, a Windows NPS server and a FortiAuthenticator are configured in the same User Group. The access-request is sent to both servers concurrently. If FortiGate receives an access-accept from either server, authentication is successful.

### To configure the internal and external interfaces:

1. Go to *Network > Interfaces*.
2. Edit the *port1* interface and set *IP/Network Mask* to *192.168.2.5/24*.
3. Edit the *port2* interface and set *IP/Network Mask* to *192.168.20.5/24*.
4. Click *OK*.

### To create a firewall address:

1. Go to *Policy & Objects > Addresses* and click *Create New > Address*.
2. Set *Name* to *192.168.20.0*.
3. Leave *Type* as *Subnet*.
4. Set *IP/Netmask* to *192.168.20.0/24*.
5. Click *OK*.

### To configure the first RADIUS server:

1. Go to *User & Device > RADIUS Servers* and click *Create New*.
2. Set *Name* to *win2k16*.
3. Leave *Authentication method* set to *Default*. The PAP, MS-CHAPv2, and CHAP methods will be tried in order.
4. Under *Primary Server*, set *IP/Name* to *192.168.20.6* and *Secret* to the shared secret configured on the RADIUS server.
5. Click *Test Connectivity* to test the connection to the server, and ensure that *Connection status* is *Successful*.
6. Click *OK*.

### To configure the second RADIUS server:

1. Go to *User & Authentication > RADIUS Servers* and click *Create New*.
2. Set *Name* to *fac*.
3. Leave *Authentication method* set to *Default*. The PAP, MS-CHAPv2, and CHAP methods will be tried in order.
4. Under *Primary Server*, set *IP/Name* to *192.168.2.71* and *Secret* to the shared secret configured on the RADIUS server.
5. Click *Test Connectivity* to test the connection to the server, and ensure that *Connection status* is *Successful*.
6. Click *OK*.

### To configure the user group:

1. Go to *User & Authentication > User Groups* and click *Create New*.
2. In the *Name* field, enter *dualPrimaryGroup*.
3. In the *Remote Groups* area, click *Add*, and from the *Remote Server* dropdown, select *fac*.
4. Click *Add* again. From the *Remote Server* dropdown select *win2k16* and click *OK*.
5. Click *OK*, and then click *OK* again.

**To configure the SSL VPN settings:**

1. Go to *VPN > SSL-VPN Settings*.
2. From the *Listen on Interface(s)* dropdown select *port1*.
3. In the *Listen on Port* field enter *10443*.
4. Optionally, from the *Server Certificate* dropdown, select the authentication certificate if you have one for this SSL VPN portal.
5. Under *Authentication/Portal Mapping*, set the default portal web-access.
  - a. Select *All Other Users/Groups* and click *Edit*.
  - b. From the *Portal* dropdown, select *web-access*.
  - c. Click *OK*.
6. Create a web portal for *PrimarySecondaryGroup*.
  - a. Under *Authentication/Portal Mapping*, click *Create New*.
  - b. Click *Users/Groups* and select *dualPrimaryGroup*.
  - c. From the *Portal* dropdown, select *full-access*.
  - d. Click *OK*.

**To configure SSL VPN firewall policy:**

1. Go to *Policy & Objects > IPv4 Policy*.
2. Click *Create New* to create a new policy, or double-click an existing policy to edit it.

<b>Name</b>	Enter the firewall policy name.
<b>Incoming Interface</b>	Select <i>SSL-VPN tunnel interface (ssl.root)</i> .
<b>Outgoing interface</b>	Set to the local network interface so that the remote user can access the internal network. For this example, select <i>port3</i> .
<b>Source</b>	<ol style="list-style-type: none"> <li>1. In the <i>Address</i> tab select <i>SSLVPN_TUNNEL_ADDR1</i>.</li> <li>2. In the <i>User</i> tab, select <i>dualPrimaryGroup</i>.</li> </ol>
<b>Destination</b>	Select the internal protected subnet <i>192.168.20.0</i> .
<b>Schedule</b>	Select <i>always</i> .
<b>Service</b>	Select <i>All</i> .
<b>Action</b>	Select <i>Accept</i> .
<b>NAT</b>	Set to <i>Enable</i> .

3. Configure any remaining firewall and security options as desired.
4. Click *OK*.

**To configure SSL VPN using the CLI:**

1. Configure the internal interface and firewall address.

```
config system interface
 edit "port3"
 set vdom "root"
 set ip 192.168.20.5 255.255.255.0
 set alias "internal"
 next
```



```
end
config firewall address
 edit "192.168.20.0"
 set uuid cc41eec2-9645-51ea-d481-5c5317f865d0
 set subnet 192.168.20.0 255.255.255.0
 next
end
```

## 2. Configure the RADIUS server.

```
config user radius
 edit "win2kl6"
 set server "192.168.20.6"
 set secret <secret>
 next
 edit "fac"
 set server "192.168.2.71"
 set secret <secret>
 next
end
```

## 3. Add the RADIUS user to the user group.

```
config user group
 edit "dualPrimaryGroup"
 set member "win2kl6" "fac"
 next
end
```

## 4. Configure SSL VPN settings.

```
config vpn ssl settings
 set servercert "server_certificate"
 set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
 set source-interface "port1"
 set source-address "all"
 set default-portal "web-access"
 config authentication-rule
 edit 1
 set groups "dualPrimaryGroup"
 set portal "full-access"
 next
 end
end
```

## 5. Configure one SSL VPN firewall policy to allow remote users to access the internal network.

```
config firewall policy
 edit 1
 set name "sslvpn-radius"
 set srcintf "ssl.root"
 set dstintf "port3"
 set srcaddr "all"
 set dstaddr "192.168.20.0"
 set groups "dualPrimaryGroup"
 set action accept
 set schedule "always"
 set service "ALL"
 set nat enable
 next
end
```

**To verify the connection:**

User *fackeith* is a member of the FortiAuthenticator server only.

User *radkeith* is a member of both the NPS server and the FortiAuthenticator server, but has different passwords on each server.

**Case 1: Connect to the SSLVPN tunnel using FortiClient with user FacAdmin:**

```
diag sniffer packet any 'port 1812' 4 0 1
interfaces=[any]
filters=[port 1812]
2020-05-15 17:21:31.217985 port3 out 192.168.20.5.11490 -> 192.168.20.6.1812: udp 118
2020-05-15 17:21:31.218091 port1 out 192.168.2.5.11490 -> 192.168.2.71.1812: udp 118
2020-05-15 17:21:31.219314 port3 in 192.168.20.6.1812 -> 192.168.20.5.11490: udp 20 <--
 access-reject
2020-05-15 17:21:31.219519 port3 out 192.168.20.5.11490 -> 192.168.20.6.1812: udp 182
2020-05-15 17:21:31.220219 port3 in 192.168.20.6.1812 -> 192.168.20.5.11490: udp 42
2020-05-15 17:21:31.220325 port3 out 192.168.20.5.11490 -> 192.168.20.6.1812: udp 119
2020-05-15 17:21:31.220801 port3 in 192.168.20.6.1812 -> 192.168.20.5.11490: udp 20
2020-05-15 17:21:31.236009 port1 in 192.168.2.71.1812 -> 192.168.2.5.11490: udp 20 <--
 access-accept
```

Access is denied by the NPS server because the user does not exist. However, access is accepted by FortiAuthenticator. The end result is the authentication is successful.

```
get vpn ssl monitor
SSL VPN Login Users:
```

Index in/out	User HTTPS	Group in/out	Auth Type	Timeout	From	HTTP
0	fackeith	dualPrimaryGroup	2(1)	292	192.168.2.202	0/0

```
SSL VPN sessions:
```

Index Tunnel/Dest	User IP	Group	Source IP	Duration	I/O Bytes
0	fackeith	dualPrimaryGroup	192.168.2.202	149	70236/4966

**Case 2: Connect to the SSLVPN tunnel using FortiClient with user radkeith:**

```
diag sniffer packet any 'port 1812' 4 0 1
interfaces=[any]
filters=[port 1812]
2020-05-15 17:26:07.335791 port1 out 192.168.2.5.17988 -> 192.168.2.71.1812: udp 118
2020-05-15 17:26:07.335911 port3 out 192.168.20.5.17988 -> 192.168.20.6.1812: udp 118
2020-05-15 17:26:07.337659 port3 in 192.168.20.6.1812 -> 192.168.20.5.17988: udp 20 <--
 access-accept
2020-05-15 17:26:07.337914 port3 out 192.168.20.5.17988 -> 192.168.20.6.1812: udp 182
2020-05-15 17:26:07.339451 port3 in 192.168.20.6.1812 -> 192.168.20.5.17988: udp 228
2020-05-15 17:26:08.352597 port1 in 192.168.2.71.1812 -> 192.168.2.5.17988: udp 20 <--
 access-reject
```

There is a password mismatch for this user on the Secondary RADIUS server. However, even though the authentication was rejected by FortiAuthenticator, it was accepted by Windows NPS. Therefore, the end result is authentication successful.

```
get vpn ssl monitor
```

## SSL VPN Login Users:

Index in/out	User HTTPS	Group in/out	Auth Type	Timeout	From	HTTP
0 0/0	radkeith	dualPrimaryGroup	2 (1)	290	192.168.2.202	0/0

## SSL VPN sessions:

Index Tunnel/Dest IP	User	Group	Source IP	Duration	I/O Bytes
0 10.212.134.200	radkeith	dualPrimaryGroup	192.168.2.202	142	64875/4966

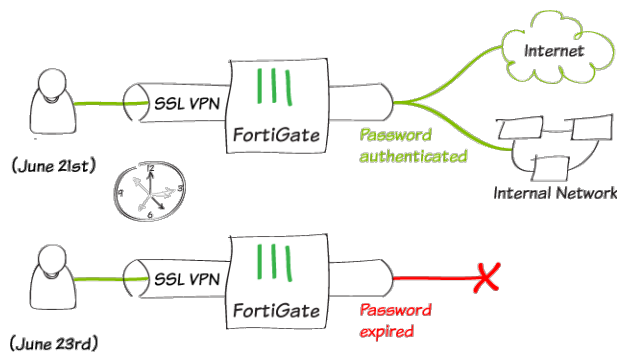
## SSL VPN with local user password policy

This is a sample configuration of SSL VPN for users with passwords that expire after two days. Users are warned after one day about the password expiring. The password policy can be applied to any local user password. The password policy cannot be applied to a user group or a local remote user such as LDAP/RADIUS/TACACS+.

In FortiOS 6.2, users are warned after one day about the password expiring and have one day to renew it. If the password expires, the user cannot renew the password and must contact the administrator for assistance.

In FortiOS 6.0/5.6, users are warned after one day about the password expiring and have to renew it. If the password expires, the user can still renew the password.

### Sample topology



### Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface.

#### To configure SSL VPN using the GUI:

1. Configure the interface and firewall address. The port1 interface connects to the internal network.
  - a. Go to *Network > Interfaces* and edit the *wan1* interface.
  - b. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.
  - c. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.

- d. Click *OK*.
- e. Go to *Policy & Objects > Address* and create an address for internet subnet *192.168.1.0*.
2. Configure user and user group.
  - a. Go to *User & Device > User Definition* to create a local user.
  - b. Go to *User & Device > User Groups* to create a user group and add that local user to it.
3. Configure and assign the password policy using the CLI.
  - a. Configure a password policy that includes an expiry date and warning time. The default start time for the password is the time the user was created.
 

```
config user password-policy
 edit "pwpolicy1"
 set expire-days 2
 set warn-days 1
 next
end
```
  - b. Assign the password policy to the user you just created.
 

```
config user local
 edit "sslvpnuser1"
 set type password
 set passwd-policy "pwpolicy1"
 next
end
```
4. Configure SSL VPN web portal.
  - a. Go to *VPN > SSL-VPN Portals* to edit the *full-access* portal.  
This portal supports both web and tunnel mode.
  - b. Disable *Enable Split Tunneling* so that all SSL VPN traffic goes through the FortiGate.
5. Configure SSL VPN settings.
  - a. Go to *VPN > SSL-VPN Settings*.
  - b. Select the *Listen on Interface(s)*, in this example, *wan1*.
  - c. Set *Listen on Port* to *10443*.
  - d. Set *Server Certificate* to the authentication certificate.
  - e. Under *Authentication/Portal Mapping*, set default Portal *web-access* for *All Other Users/Groups*.
  - f. Create new *Authentication/Portal Mapping* for group *sslvpngroup* mapping portal *full-access*.
6. Configure SSL VPN firewall policy.
  - a. Go to *Policy & Objects > IPv4 Policy*.
  - b. Fill in the firewall policy name. In this example, *sslvpn certificate auth*.
  - c. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.
  - d. Set the *Source Address* to *all* and *Source User* to *sslvpngroup*.
  - e. Set the *Outgoing Interface* to the local network interface so that the remote user can access the internal network. In this example, *port1*.
  - f. Set *Destination Address* to the internal protected subnet *192.168.1.0*.
  - g. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.
  - h. Enable *NAT*.
  - i. Configure any remaining firewall and security options as desired.
  - j. Click *OK*.

**To configure SSL VPN using the CLI:****1. Configure the interface and firewall address.**

```
config system interface
 edit "wan1"
 set vdom "root"
 set ip 172.20.120.123 255.255.255.0
 next
end
```

**2. Configure internal interface and protected subnet, then connect the port1 interface to the internal network.**

```
config system interface
 edit "port1"
 set vdom "root"
 set ip 192.168.1.99 255.255.255.0
 next
end

config firewall address
 edit "192.168.1.0"
 set subnet 192.168.1.0 255.255.255.0
 next
end
```

**3. Configure user and user group.**

```
config user local
 edit "sslvpnuser1"
 set type password
 set passwd your-password
 next
end

config user group
 edit "sslvpngroup"
 set member "vpnuser1"
 next
end
```

**4. Configure and assign the password policy.**

- a. Configure a password policy that includes an expiry date and warning time. The default start time for the password is the time the user was created.**

```
config user password-policy
 edit "pwpolicy1"
 set expire-days 2
 set warn-days 1
 next
end
```

- b. Assign the password policy to the user you just created.**

```
config user local
 edit "sslvpnuser1"
 set type password
 set passwd-policy "pwpolicy1"
 next
end
```

**5. Configure SSL VPN web portal.**

```
config vpn ssl web portal
 edit "full-access"
 set tunnel-mode enable
 set web-mode enable
 set ip-pools "SSLVPN_TUNNEL_ADDR1"
 set split-tunneling disable
 next
end
```

**6. Configure SSL VPN settings.**

```
config vpn ssl settings
 set servercert "server_certificate"
 set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
 set source-interface "wan1"
 set source-address "all"
 set default-portal "web-access"
 config authentication-rule
 edit 1
 set groups "sslvpngroup"
 set portal "full-access"
 next
 end
end
```

**7. Configure one SSL VPN firewall policy to allow remote user to access the internal network.**

```
config firewall policy
 edit 1
 set name "sslvpn web mode access"
 set srcintf "ssl.root"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "192.168.1.0"
 set groups "sslvpngroup"
 set action accept
 set schedule "always"
 set service "ALL"
 set nat enable
 next
end
```

**To see the results of web portal:**

1. From a remote device, use a web browser to log into the SSL VPN web portal <http://172.20.120.123:10443>.
2. Log in using the *sslvpnuser1* credentials.  
When the warning time is reached, the user is prompted to enter a new password.  
In FortiOS 6.2, when the password expires, the user cannot renew the password and must contact the administrator.  
In FortiOS 6.0/5.6, when the password expires, the user can still renew the password.
3. On the FortiGate, go to *Monitor > SSL-VPN Monitor* to confirm the user connection.

**To see the results of tunnel connection:**

1. Download FortiClient from [www.forticlient.com](http://www.forticlient.com).
2. Open the FortiClient Console and go to *Remote Access > Configure VPN*.
3. Add a new connection.
  - Set the connection name.
  - Set *Remote Gateway* to the IP of the listening FortiGate interface, in this example, *172.20.120.123*.
4. Select *Customize Port* and set it to *10443*.
5. Save your settings.
6. Log in using the *sslvpnuser1* credentials.  
When the warning time is reached, the user is prompted to enter a new password.

**To check the SSL VPN connection using the GUI:**

1. Go to *VPN > Monitor > SSL-VPN Monitor* to verify the user's connection.
2. Go to *Log & Report > Forward Traffic* to view the details of the SSL VPN traffic.

**To check that login failed due to password expired on GUI:**

1. Go to *Log & Report > Events* and select *VPN Events* from the event type dropdown list to see the SSL VPN alert labeled *ssl-login-fail*.
2. Click *Details* to see the log details about the *Reason* *sslvpn\_login\_password\_expired*.

**To check the web portal login using the CLI:**

```
get vpn ssl monitor
SSL VPN Login Users:
```

Index	User	Auth Type	Timeout	From	HTTP in/out	HTTPS in/out
0	sslvpnuser1	1 (1)	229	10.1.100.254	0/0	0/0

```
SSL VPN sessions:
```

Index	User	Source IP	Duration	I/O Bytes	Tunnel/Dest IP
-------	------	-----------	----------	-----------	----------------

**To check the tunnel login using the CLI:**

```
get vpn ssl monitor
SSL VPN Login Users:
```

Index	User	Auth Type	Timeout	From	HTTP in/out	HTTPS in/out
0	sslvpnuser1	1 (1)	291	10.1.100.254	0/0	0/0

```
SSL VPN sessions:
```

Index	User	Source IP	Duration	I/O Bytes	Tunnel/Dest IP
0	sslvpnuser1	10.1.100.254	9	22099/43228	10.212.134.200

**To check the FortiOS 6.2 login password expired event log:**

```
FG201E4Q17901354 # execute log filter category event
FG201E4Q17901354 # execute log filter field subtype vpn
FG201E4Q17901354 # execute log filter field action ssl-login-fail
```

```
FG201E4Q17901354 # execute log display
1: date=2019-02-15 time=10:57:56 logid="0101039426" type="event" subtype="vpn" level="alert"
vd="root" eventtime=1550257076 logdesc="SSL VPN login fail" action="ssl-login-fail"
tunneltype="ssl-web" tunnelid=0 remip=10.1.100.254 user="u1" group="g1" dst_host="N/A"
reason="sslvpn_login_password_expired" msg="SSL user failed to logged in"
```

## SSL VPN with certificate authentication

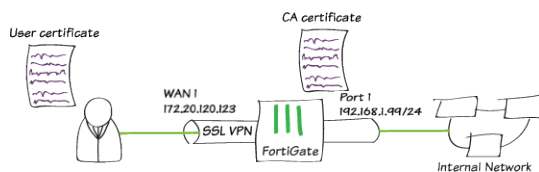
This is an example configuration of SSL VPN that requires users to authenticate using a client certificate. In this example, the server and client certificates are signed by the same Certificate Authority (CA).



Self-signed certificates are provided by default to simplify initial installation and testing. It is **HIGHLY** recommended that you acquire a signed certificate for your installation.

Continuing to use these certificates can result in your connection being compromised, allowing attackers to steal your information, such as credit card details.

For more information, please review the [Use a non-factory SSL certificate for the SSL VPN portal on page 1372](#) and learn how to [Procure and import a signed SSL certificate on page 741](#).



## Configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface.

### To configure SSL VPN using the GUI:

1. Configure the interface and firewall address. The port1 interface connects to the internal network.
  - a. Go to *Network > Interfaces* and edit the *wan1* interface.
  - b. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.
  - c. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.
  - d. Click OK.
  - e. Go to *Policy & Objects > Address* and create an address for the internal subnet *192.168.1.0*.
2. Install the server certificate. The server certificate is used for authentication and for encrypting SSL VPN traffic.
  - a. Go to *System > Feature Visibility* and ensure *Certificates* is enabled.
  - b. Go to *System > Certificates* and select *Import > Local Certificate*.
    - Set *Type* to *Certificate*.
    - Choose the *Certificate file* and the *Key file* for your certificate, and enter the *Password*.
    - If required, you can change the *Certificate Name*.

The server certificate now appears in the list of *Certificates*.

3. Install the CA certificate.

The CA certificate is the certificate that signed both the server certificate and the user certificate. In this example, it is used to authenticate SSL VPN users.



- a. Go to *System > Certificates* and select *Import > CA Certificate*.
- b. Select *Local PC* and then select the certificate file.

The CA certificate now appears in the list of *External CA Certificates*. In this example, it is called *CA\_Cert\_1*.

#### 4. Configure PKI users and a user group.

To use certificate authentication, use the CLI to create PKI users.

```
config user peer
 edit pki01
 set ca CA_Cert_1
 set subject "CN=User01"
 next
end
```

Ensure that the subject matches the name of the user certificate. In this example, *User01*.

When you have create a PKI user, a new menu is added to the GUI.

- a. Go to *User & Device > PKI* to see the new user.
  - b. Edit the user account and expand *Two-factor authentication*.
  - c. Enable *Require two-factor authentication* and set a password for the account.
  - d. Go to *User & Device > User > User Groups* and create a group *sslvpngroup*.
  - e. Add the PKI user *pki01* to the group.
- #### 5. Configure SSL VPN web portal.
- a. Go to *VPN > SSL-VPN Portals* to edit the *full-access* portal.  
This portal supports both web and tunnel mode.
  - b. Disable *Enable Split Tunneling* so that all SSL VPN traffic goes through the FortiGate.
- #### 6. Configure SSL VPN settings.
- a. Go to *VPN > SSL-VPN Settings*.
  - b. Select the *Listen on Interface(s)*, in this example, *wan1*.
  - c. Set *Listen on Port* to *10443*.
  - d. Set *Server Certificate* to the authentication certificate.
  - e. Enable *Require Client Certificate*.
  - f. Under *Authentication/Portal Mapping*, set default Portal *web-access* for *All Other Users/Groups*.
  - g. Create new *Authentication/Portal Mapping* for group *sslvpngroup* mapping portal *full-access*.
- #### 7. Configure SSL VPN firewall policy.
- a. Go to *Policy & Objects > IPv4 Policy*.
  - b. Fill in the firewall policy name. In this example, *sslvpn certificate auth*.
  - c. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.
  - d. Set the *Source Address* to *all* and *Source User* to *sslvpngroup*.
  - e. Set the *Outgoing Interface* to the local network interface so that the remote user can access the internal network. In this example, *port1*.
  - f. Set *Destination Address* to the internal protected subnet *192.168.1.0*.
  - g. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.
  - h. Enable *NAT*.
  - i. Configure any remaining firewall and security options as desired.
  - j. Click *OK*.

**To configure SSL VPN using the CLI:****1. Configure the interface and firewall address.**

```
config system interface
 edit "wan1"
 set vdom "root"
 set ip 172.20.120.123 255.255.255.0
 next
end
```

**2. Configure internal interface and protected subnet., then connect the port1 interface to the internal network.**

```
config system interface
 edit "port1"
 set vdom "root"
 set ip 192.168.1.99 255.255.255.0
 next
end
config firewall address
 edit "192.168.1.0"
 set subnet 192.168.1.0 255.255.255.0
 next
end
```

**3. Install the server certificate.**

The server certificate is used for encrypting SSL VPN traffic and will be used for authentication. While it is easier to install the server certificate from GUI, the CLI can be used to import a p12 certificate from a TFTP server.

To import a p12 certificate, put the certificate *server\_certificate.p12* on your TFTP server, then run following command on the FortiGate:

```
execute vpn certificate local import tftp server_certificate.p12 <your tftp_server> p12
<your password for PKCS12 file>
```

To check that the server certificate is installed:

```
show vpn certificate local server_certificate
```

**4. Install the CA certificate.**

The CA certificate is the certificate that signed both the server certificate and the user certificate. In this example, it is used to authenticate SSL VPN users. While it is easier to install the CA certificate from GUI, the CLI can be used to import a CA certificates from a TFTP server.

To import a CA certificate, put the CA certificate on your TFTP server, then run following command on the FortiGate:

```
execute vpn certificate ca import tftp <your CA certificate name> <your tftp server>
```

To check that a new CA certificate is installed:

```
show vpn certificate ca
```

**5. Configure PKI users and a user group.**

```
config user peer
 edit pki01
 set ca CA_Cert_1
 set subject "CN=User01"
 set two-factor enable
 set passwd <your-password>
 next
```

```
end
config user group
 edit "sslvpngroup"
 set member "pki01"
 next
end
```

#### 6. Configure SSL VPN web portal.

```
config vpn ssl web portal
 edit "full-access"
 set tunnel-mode enable
 set web-mode enable
 set ip-pools "SSLVPN_TUNNEL_ADDR1"
 set split-tunneling disable
 next
end
```

#### 7. Configure SSL VPN settings.

```
config vpn ssl settings
 set servercert "server_certificate"
 set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
 set source-interface "wan1"
 set source-address "all"
 set default-portal "web-access"
 set reqclientcert enable
 config authentication-rule
 edit 1
 set groups "sslvpngroup"
 set portal "full-access"
 next
 end
end
```

#### 8. Configure one SSL VPN firewall policy to allow remote user to access the internal network.

```
config firewall policy
 edit 1
 set name "sslvpn web mode access"
 set srcintf "ssl.root"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "192.168.1.0"
 set groups "sslvpngroup"
 set action accept
 set schedule "always"
 set service "ALL"
 set nat enable
 next
end
```

## Installation

To use the user certificate, you must first install it on the user's PC. When the user tries to authenticate, the user certificate is checked against the CA certificate to verify that they match.

Every user should have a unique user certificate. This allows you to distinguish each user and revoke a specific user's certificate, such as if a user no longer has VPN access.

#### To install the user certificate on Windows 7, 8, and 10:

1. Double-click the certificate file to open the *Import Wizard*.
2. Use the *Import Wizard* to import the certificate into the *Personal store* of the current user.

#### To install the user certificate on Mac OS X:

1. Open the certificate file, to open *Keychain Access*.
2. Double-click the certificate.
3. Expand *Trust* and select *Always Trust*.

#### To see the results of tunnel connection:

1. Download FortiClient from [www.forticlient.com](http://www.forticlient.com).
2. Open the FortiClient Console and go to *Remote Access > Configure VPN*.
3. Add a new connection.
  - Set *VPN Type* to *SSL VPN*.
  - Set *Remote Gateway* to the IP of the listening FortiGate interface, in this example, *172.20.120.123*.
4. Select *Customize Port* and set it to *10443*.
5. Enable *Client Certificate* and select the authentication certificate.
6. Save your settings.
7. Use the credentials you've set up to connect to the SSL VPN tunnel.  
If the certificate is correct, you can connect.

#### To see the results of web portal:

1. In a web browser, log into the portal *http://172.20.120.123:10443*.  
A message requests a certificate for authentication.
2. Select the user certificate.
3. Enter your user credentials.  
If the certificate is correct, you can connect to the SSL VPN web portal.

#### To check the SSL VPN connection using the GUI:

1. Go to *VPN > Monitor > SSL-VPN Monitor* to verify the list of SSL users.
2. Go to *Log & Report > Events* and select *VPN Events* from the event type dropdown list to view the details for the SSL connection log.

#### To check the SSL VPN connection using the CLI:

```
get vpn ssl monitor
```

```
SSL VPN Login Users:
```

Index	User	Auth Type	Timeout	From	HTTP in/out	HTTPS in/out
0	pki01,cn=User01		1 (1)	229	10.1.100.254	0/0 0/0
1	pki01,cn=User01		1 (1)	291	10.1.100.254	0/0 0/0

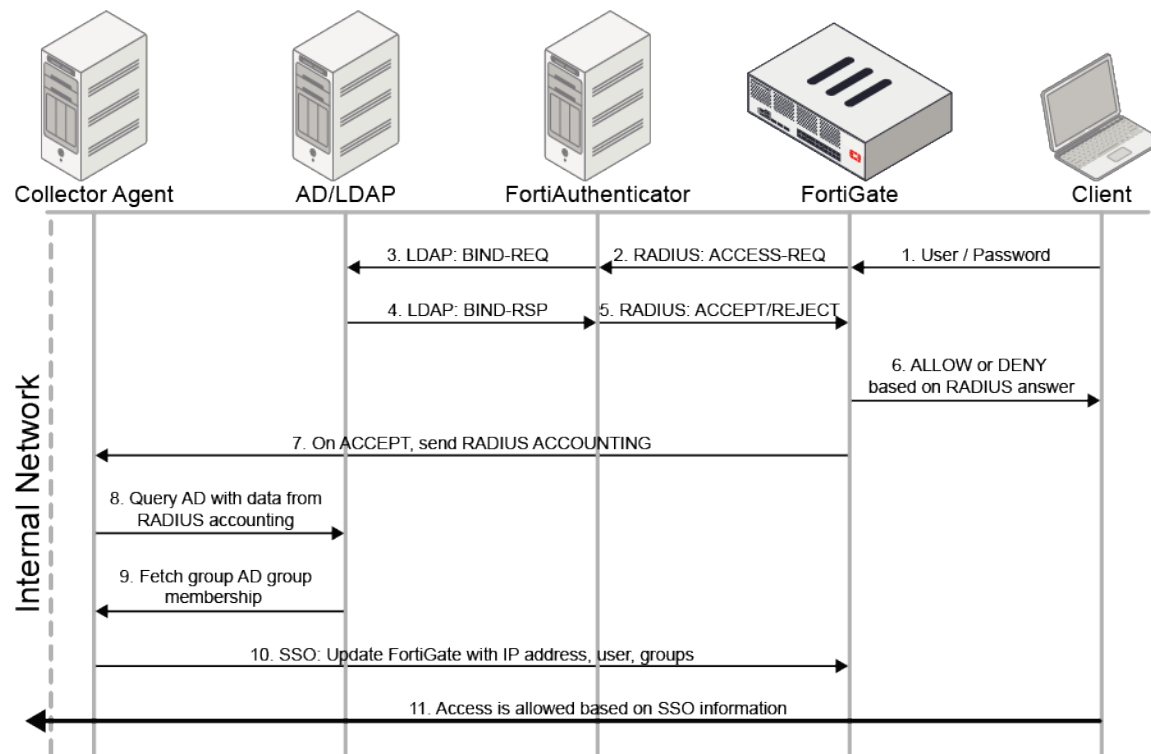
```
SSL VPN sessions:
```

Index	User	Source IP	Duration	I/O Bytes	Tunnel/Dest IP
0	pki01,cn=User01	10.1.100.254	9	22099/43228	10.212.134.200

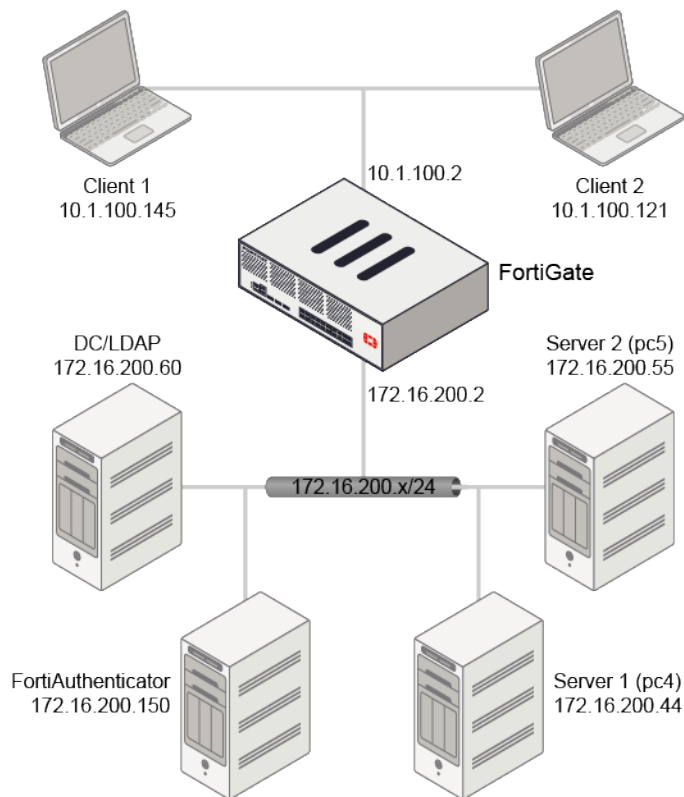
## Dynamic address support for SSL VPN policies

Dynamic SSO user groups can be used in place of address objects when configuring SSL VPN policies. This allows dynamic IP addresses to be used in SSL VPN policies. A remote user group can be used for authentication while an FSSO group is separately used for authorization. Using a dummy policy for remote user authentication and a policy for FSSO group authorization, FSSO can be used with SSL VPN tunnels

This image shows the authentication and authorization flow:



In this example, FortiAuthenticator is used as a RADIUS server. It uses a remote AD/LDAP server for authentication, then returns the authentication results to the FortiGate. This allows the client to have a dynamic IP address after successful authentication.



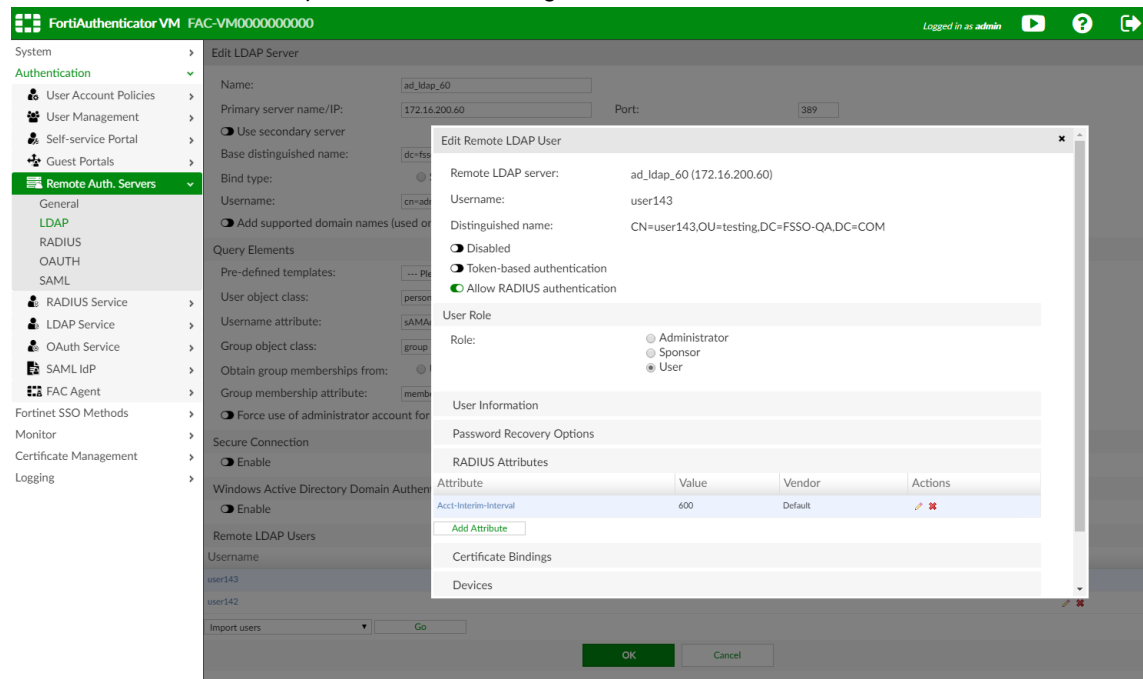
First, on the LDAP server, create two users each in their own group, *user142* in group *pc\_group1*, and *user143* in group *pc\_group2*.

## Configure the FortiAuthenticator

To add a remote LDAP server and users on the FortiAuthenticator:

1. Go to *Authentication > Remote Auth. Servers > LDAP*.
2. Click *Create New*.
3. Set the following:
  - *Name*: *ad\_ldap\_60*
  - *Primary server name/IP*: *172.16.200.60*
  - *Base distinguished name*: *dc=fsso-qa,dc=com*
  - *Bind type*: *Regular*
  - *Username*: *cn=administrator,cn=User*
  - *Password*: <enter a password>
4. Click *OK*.
5. Edit the new LDAP server.
6. Import the remote LDAP users.
7. Edit each user to confirm that they have the RADIUS attribute *Acct-Interim-Interval*. This attribute is used by

FortiGate to send interim update account messages to the RADIUS server.



**To create a RADIUS client for FortiGate as a remote authentication server:**

1. Go to *Authentication > RADIUS Service > Clients*.
2. Click *Create New*.
3. Set the following:
  - *Name*: `fsso_ldap`
  - *Client address*: Range `172.16.200.1~172.16.200.10`
  - *Secret*: <enter a password>
4. In the *Realms* table, set the realm to the LDAP server that was just added: `ad_ldap_60`.
5. Click *OK*.

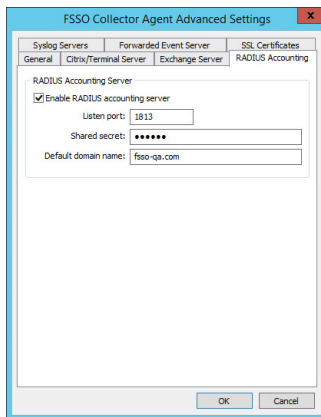
FortiAuthenticator can now be used as a RADIUS server, and the authentication credentials all come from the DC/LDAP server.

## Fortinet Single Sign-On Collector Agent

**To configure the Fortinet Single Sign-On Collector Agent:**

1. Select *Require authenticated connection from FortiGate* and enter a *Password*.
2. Click *Advanced Settings*.
3. Select the *RADIUS Accounting* tab.

4. Select *Enable RADIUS accounting server* and set the *Shared secret*.



5. Click *OK*, then click *Save&close*.

The collector agent can now accept accounting requests from FortiGate, and retrieve the IP addresses and usernames of SSL VPN client from the FortiGate with accounting request messages.

## Configure the FortiGate

### To configure the FortiGate in the CLI:

1. Create a Fortinet Single Sign-On Agent fabric connector:

```
config user fsso
 edit "AD_CollectAgent"
 set server "172.16.200.60"
 set password 123456
 next
end
```

2. Add the RADIUS server:

```
config user radius
 edit "rad150"
 set server "172.16.200.150"
 set secret 123456
 set acct-interim-interval 600
 config accounting-server
 edit 1
 set status enable
 set server "172.16.200.60"
 set secret 123456
 next
 end
 next
end
```

3. Create a user group for the RADIUS server:

```
config user group
 edit "rad_group"
 set member "rad150"
 next
end
```



**4. Create user groups for each of the FSSO groups:**

```
config user group
 edit "fsso_group1"
 set group-type fsso-service
 set member "CN=PC_GROUP1,OU=TESTING,DC=FSSO-QA,DC=COM"
 next
 edit "fsso_group2"
 set group-type fsso-service
 set member "CN=PC_GROUP2,OU=TESTING,DC=FSSO-QA,DC=COM"
 next
end
```

**5. Create an SSL VPN portal and assign the RADIUS user group to it:**

```
config vpn ssl web portal
 edit "testportal"
 set tunnel-mode enable
 set ipv6-tunnel-mode enable
 set web-mode enable
 ...
 next
end
config vpn ssl settings
 ...
 set default-portal "full-access"
 config authentication-rule
 edit 1
 set groups "rad_group"
 set portal "testportal"
 next
 end
end
```

**6. Create firewall addresses:**

```
config firewall address
 edit "none"
 set subnet 0.0.0.0 255.255.255.255
 next
 edit "pc4"
 set subnet 172.16.200.44 255.255.255.255
 next
 edit "pc5"
 set subnet 172.16.200.55 255.255.255.255
 next
end
```

**7. Create one dummy policy for authentication only, and two normal policies for authorization:**

```
config firewall policy
 edit 1
 set name "sslvpn_authentication"
 set srcintf "ssl.vdom1"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "none"
 set action accept
 set schedule "always"
```

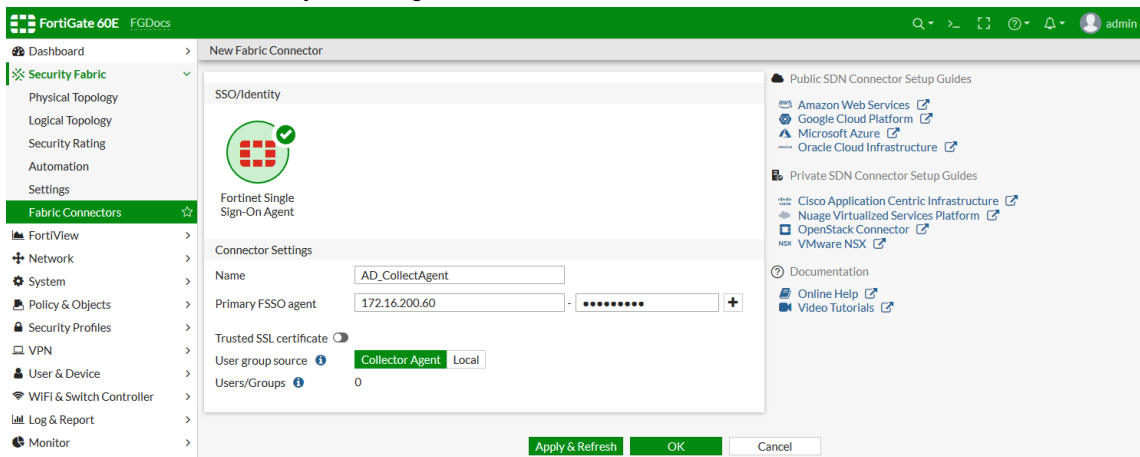
```

 set service "ALL"
 set logtraffic all
 set groups "rad_group"
 set nat enable
 next
 edit 3
 set name "sslvpn_authorization1"
 set srcintf "ssl.vdom1"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "pc4"
 set action accept
 set schedule "always"
 set service "ALL"
 set logtraffic all
 set groups "fsso_group1"
 set nat enable
 next
 edit 4
 set name "sslvpn_authorization2"
 set srcintf "ssl.vdom1"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "pc5"
 set action accept
 set schedule "always"
 set service "ALL"
 set logtraffic all
 set groups "fsso_group2"
 set nat enable
 next
end

```

### To create an FSSO agent fabric connector in the GUI:

1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New*.
3. Click *Fortinet Single Sign-On Agent*.
4. Enter the name and *Primary FSSO agent* information.



5. Click *Apply & Refresh*.

The FSSO groups are retrieved from the collector agent.

**To add the RADIUS server in the GUI:**

1. Go to *User & Device > RADIUS Servers*.
2. Click *Create New*.
3. Enter a name for the server.
4. Enter the *IP/Name* and *Secret* for the primary server.
5. Click *Test Connectivity* to ensure that there is a successful connection.

6. Click *OK*.

7. Configure an accounting server with the following CLI command:

```
config user radius
edit rad150
set acct-interim-interval 600
config accounting-server
edit 1
set status enable
set server 172.16.200.60
set secret *****
next
end
next
end
```

**To create a user group for the RADIUS server in the GUI:**

1. Go to *User & Device > User Groups*.
2. Click *Create New*.
3. Enter a name for the group and set the *Type* to *Firewall*.

#### 4. Add the RADIUS server as a remote group.

FortiGate 60E FGDocs

Dashboard > New User Group

Security Fabric >

FortiView >

Network >

System >

Policy & Objects >

Security Profiles >

VPN >

User & Device >

User Definition >

User Groups ☆

Guest Management >

Device Inventory >

LDAP Servers >

RADIUS Servers >

Authentication Settings >

FortiTokens >

WiFi & Switch Controller >

Log & Report >

Monitor >

Name: rad\_group

Type: Firewall

Members: +

Remote Groups

Remote Server	Group Name
rad150	

OK Cancel

#### 5. Click OK.

### To create user groups for each of the FSSO groups in the GUI:

1. Go to *User & Device > User Groups*.
2. Click *Create New*.
3. Enter a name for the group and set the *Type* to *Fortinet Single Sign-On (FSSO)*.
4. Add PC\_GROUP1 as a member:

CN=PC\_GROUP1,OU=TESTING,DC=FSSO-QA,DC=COM

FortiGate 60E FGDocs

User & Device >

User Definition >

User Groups ☆

Guest Management >

Device Inventory >

LDAP Servers >

RADIUS Servers >

Authentication Settings >

FortiTokens >

WiFi & Switch Controller >

Log & Report >

Name: fss\_group1

Type: Fortinet Single Sign-On (FSSO)

Members: CN=PC\_GROUP1,OU=TESTING,DC=FSSO-QA,DC=COM

OK Cancel

#### 5. Click OK.

#### 6. Add a second user group with PC\_GROUP2 as a member:

CN=PC\_GROUP2,OU=TESTING,DC=FSSO-QA,DC=COM

FortiGate 60E FGDocs

User & Device >

User Definition >

User Groups ☆

Guest Management >

Device Inventory >

LDAP Servers >

RADIUS Servers >

Authentication Settings >

FortiTokens >

WiFi & Switch Controller >

Log & Report >

Name: fss\_group2

Type: Fortinet Single Sign-On (FSSO)

Members: CN=PC\_GROUP2,OU=TESTING,DC=FSSO-QA,DC=COM

OK Cancel

#### 7. Click OK.

### To create an SSL VPN portal and assign the RADIUS user group to it in the GUI:

1. Go to *VPN > SSL VPN Portals*.
2. Click *Create New*.
3. Configure the portal, then click *OK*.
4. Go to *VPN > SSL VPN Settings*.
5. Configure the required settings.
6. Create an *Authentication/Portal Mapping* table entry:
  - a. Click *Create New*.
  - b. Set *User/Groups* to *rad\_group*.
  - c. Set *Portal* to *testportal*.
  - d. Click *OK*.
7. Click *OK*.

### To create policies for authentication and authorization in the GUI:

1. Go to *Policy & Object > IPv4 Policy*.
2. Configure a dummy policy for authentication. Set the destination to *none* so that traffic is not allowed through the FortiGate, and add *rad\_group* as a source.
3. Configure two authorization policies, with the FSSO groups as sources.

ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
1	sslvpn_authentication	sslvdn1	port1	all rad_group	none	always	ALL	ACCEPT	Enabled	SSL no-inspection	All
3	sslvpn_authorization1	sslvdn1	port1	all fsso_group1	pc4	always	ALL	ACCEPT	Enabled	SSL no-inspection	All
4	sslvpn_authorization2	sslvdn1	port1	all fsso_group2	pc5	always	ALL	ACCEPT	Enabled	SSL no-inspection	All
0	Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled

## Confirmation

On *Client 1*, log in to FortiClient using *user142*. Traffic can go to *pc4* (172.16.200.44), but cannot go to *pc5* (172.16.200.55).

On *Client 2*, log in to FortiClient using *user143*. Traffic can go to *pc5* (172.16.200.55), but cannot go to *pc4* (172.16.200.44).

On the FortiGate, check the authenticated users list and the SSL VPN status:

```
diagnose firewall auth list
```

```
10.212.134.200, USER142
 type: fsso, id: 0, duration: 173, idled: 173
 server: AD_CollectAgent
 packets: in 0 out 0, bytes: in 0 out 0
 user_id: 16777229
 group_id: 3 33554434
 group_name: fsso_group1 CN=PC_GROUP1,OU=TESTING,DC=FSO-QA,DC=COM
```

```
10.212.134.200, user142
```

```

type: fw, id: 0, duration: 174, idled: 174
expire: 259026, allow-idle: 259200
flag(80): sslvpn
server: rad150
packets: in 0 out 0, bytes: in 0 out 0
group_id: 4
group_name: rad_group

10.212.134.201, USER143
type: fsso, id: 0, duration: 78, idled: 78
server: AD_CollectAgent
packets: in 0 out 0, bytes: in 0 out 0
group_id: 1 33554435
group_name: fsso_group2 CN=PC_GROUP2,OU=TESTING,DC=FSSO-QA,DC=COM

10.212.134.201, user143
type: fw, id: 0, duration: 79, idled: 79
expire: 259121, allow-idle: 259200
flag(80): sslvpn
server: rad150
packets: in 0 out 0, bytes: in 0 out 0
group_id: 4
group_name: rad_group

----- 4 listed, 0 filtered -----

get vpn ssl monitor
SSL VPN Login Users:
 Index User Auth Type Timeout From HTTP in/out HTTPS in/out
 0 user142 2(1) 600 10.1.100.145 0/0 0/0
 1 user143 2(1) 592 10.1.100.254 0/0 0/0

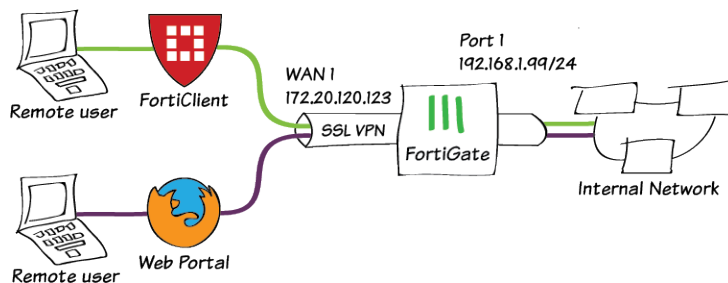
SSL VPN sessions:
 Index User Source IP Duration I/O Bytes Tunnel/Dest IP
 0 user142 10.1.100.145 104 32190/16480 10.212.134.200
 1 user143 10.1.100.254 11 4007/4966 10.212.134.201

```

## SSL VPN multi-realm

This sample shows how to create a multi-realm SSL VPN that provides different portals for different user groups.

### Sample topology



## Sample configuration

WAN interface is the interface connected to ISP. This example shows static mode. You can also use DHCP or PPPoE mode. The SSL VPN connection is established over the WAN interface.



The split tunneling routing address cannot use an FQDN or an address group that includes an FQDN.

### To configure SSL VPN using the GUI:

1. Configure the interface and firewall address. The port1 interface connects to the internal network.
  - a. Go to *Network > Interfaces* and edit the *wan1* interface.
  - b. Set *IP/Network Mask* to *172.20.120.123/255.255.255.0*.
  - c. Edit *port1* interface and set *IP/Network Mask* to *192.168.1.99/255.255.255.0*.
  - d. Click OK.
  - e. Go to *Policy & Objects > Address* and create an address for internet *QA\_subnet* with subnet *192.168.1.0/24* and *HR\_subnet* with subnet *10.1.100.0/24*.
2. Configure user and user group.
  - a. Go to *User & Device > User Definition* to create local users *qa-user1* and *hr-user1*.
  - b. Go to *User & Device > User Groups* to create separate user groups for web-only and full-access portals:
    - *QA\_group* with member *qa-user1*.
    - *HR\_group* with the member *hr-user1*.
3. Configure SSL VPN web portal.
  - a. Go to *VPN > SSL-VPN Portals* to create portal *qa-tunnel*.
  - b. Enable *Tunnel Mode*.
  - c. Create a portal *hr-web* with *Web Mode* enabled.
4. Configure SSL VPN realms.
  - a. Go to *System > Feature Visibility* to enable *SSL-VPN Realms*.
  - b. Go to *VPN > SSL-VPN Realms* to create realms for *qa* and *hr*.
  - c. (Optional) To access each realm with FQDN instead of the default URLs *https://172.20.120.123:10443/hr* and *https://172.20.120.123:10443/qa*, you can configure a virtual-host for the realm in the CLI.
 

```
config vpn ssl web realm
 edit hr
 set virtual-host hr.mydomain.com
 next
 edit qa
 set virtual-host qa.mydomain.com
 next
end
```

Where *mydomain.com* is the name of your domain. Ensure FQDN resolves to the FortiGate wan1 interface and that your certificate is a wildcard certificate.
5. Configure SSL VPN settings.
  - a. Go to *VPN > SSL-VPN Settings*.
  - b. For *Listen on Interface(s)*, select *wan1*.
  - c. Set *Listen on Port* to *10443*.
  - d. Choose a certificate for *Server Certificate*. The default is *Fortinet\_Factory*.

- e. In *Authentication/Portal Mapping All Other Users/Groups*, set the *Portal* to *web-access*.
- f. Create new *Authentication/Portal Mapping* for group *QA\_group* mapping portal *qa-tunnel*.
- g. Specify the realm *qa*.
- h. Add another entry for group *HR\_group* mapping portal *hr-web*.
- i. Specify the realm *hr*.
- 6. Configure SSL VPN firewall policy.
  - a. Go to *Policy & Objects > IPv4 Policy*.
  - b. Create a firewall policy for QA access.
  - c. Fill in the firewall policy name. In this example, *QA sslvpn tunnel mode access*.
  - d. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.
  - e. Choose an *Outgoing Interface*. In this example, *port1*.
  - f. Set the *Source* to *all* and group to *QA\_group*.
  - g. In this example, the *Destination* is the internal protected subnet *QA\_subnet*.
  - h. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.
  - i. Click OK.
  - j. Create a firewall policy for HR access.
  - k. Fill in the firewall policy name. In this example, *HR sslvpn web mode access*.
  - l. Incoming interface must be *SSL-VPN tunnel interface(ssl.root)*.
  - m. Choose an *Outgoing Interface*. In this example, *port1*.
  - n. Set the *Source* to *all* and group to *HR\_group*.
  - o. In this example, the *Destination* is the internal protected subnet *HR\_subnet*.
  - p. Set *Schedule* to *always*, *Service* to *ALL*, and *Action* to *Accept*.
  - q. Click OK.

### To configure SSL VPN using the CLI:

1. Configure the interface and firewall address.

```
config system interface
 edit "wan1"
 set vdom "root"
 set ip 172.20.120.123 255.255.255.0
 next
end
```

2. Configure internal interface and protected subnet, then connect the port1 interface to the internal network.

```
config system interface
 edit "port1"
 set vdom "root"
 set ip 192.168.1.99 255.255.255.0
 next
end

config firewall address
 edit "QA_subnet"
 set subnet 192.168.1.0 255.255.255.0
 next
 edit "HR_subnet"
 set subnet 10.1.100.0 255.255.255.0
```



```
 next
end
```

### 3. Configure user and user group.

```
config user local
 edit "qa_user1"
 set type password
 set passwd your-password
 next
end
config user group
 edit "QA_group"
 set member "qa_user1"
 next
end

config user local
 edit "hr_user1"
 set type password
 set passwd your-password
 next
end
config user group
 edit "HR_group"
 set member "hr_user1"
 next
end
```

### 4. Configure SSL VPN web portal.

```
config vpn ssl web portal
 edit "qa-tunnel"
 set tunnel-mode enable
 set ip-pools "SSLVPN_TUNNEL_ADDR1"
 set split-tunneling enable
 set split-tunneling-routing-address "QA_subnet"
 next
end

config vpn ssl web portal
 edit "hr-web"
 set web-mode enable
 next
end
```

### 5. Configure SSL VPN realms.

```
config vpn ssl web realm
 edit hr
 set virtual-host hr.mydomain.com
 next
 edit qa
 set virtual-host qa.mydomain.com
 next
end
```

The `set virtual-host` setting is optional. For example:

```
config vpn ssl web realm
 edit hr
 next
```

```
 edit qa
 next
end
```

## 6. Configure SSL VPN settings.

```
config vpn ssl settings
 set servercert "Fortinet_Factory"
 set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
 set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
 set source-interface "wan1"
 set source-address "all"
 set source-address6 "all"
 set default-portal "full-access"
 config authentication-rule
 edit 1
 set groups "QA_group"
 set portal "qa-tunnel"
 set realm qa
 next
 edit 2
 set groups "HR_group"
 set portal "hr-web"
 set realm hr
 next
 end
end
```

## 7. Configure two SSL VPN firewall policies to allow remote QA user to access internal QA network and HR user to access HR network.

```
config firewall policy
 edit 1
 set name "QA sslvpn tunnel access"
 set srcintf "ssl.root"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "QA_subnet"
 set groups "QA_group"
 set action accept
 set schedule "always"
 set service "ALL"
 next
 edit 2
 set name "HR sslvpn web access"
 set srcintf "ssl.root"
 set dstintf "port1"
 set srcaddr "all"
 set dstaddr "HR_subnet"
 set groups "HR_group"
 set action accept
 set schedule "always"
 set service "ALL"
 next
end
```

**To see the results for QA user:**

1. Download FortiClient from [www.forticlient.com](http://www.forticlient.com).
2. Open the FortiClient Console and go to *Remote Access*.
3. Add a new connection.
  - Set *VPN Type* to *SSL VPN*.
  - Set *Remote Gateway* to *https://172.20.120.123:10443/qa.*
  - If a virtual-host is specified, use the FQDN defined for the realm (*qa.mydomain.com*).
4. Select *Customize Port* and set it to *10443*.
5. Save your settings.
6. Use the credentials you've set up to connect to the SSL VPN tunnel.  
If the user's computer has antivirus software, a connection is established; otherwise FortiClient shows a compliance warning.
7. After connection, traffic to subnet *192.168.1.0* goes through the tunnel.
8. On the FortiGate, go to *VPN > Monitor > SSL-VPN Monitor* to verify the list of SSL users.
9. On the FortiGate, go to *Log & Report > Forward Traffic* and view the details of the traffic.

**To see the results for HR user:**

1. In a web browser, log into the portal *https://172.20.120.123:10443/hr* using the credentials you've set up.
2. Alternatively, if a virtual-host is specified, use the FQDN defined for the realm (*hr.mydomain.com*).
3. Go to *VPN > Monitor > SSL-VPN Monitor* to verify the list of SSL users.
4. Go to *Log & Report > Forward Traffic* and view the details of the traffic.

## SSL VPN with Azure AD SSO integration

You can use SAML single sign on to authenticate against Azure Active Directory with SSL VPN SAML user via tunnel and web modes. See:

- [Configuring SAML SSO login for SSL VPN with Azure AD acting as SAML IdP](#)
- [Tutorial: Azure AD SSO integration with FortiGate SSL VPN](#)

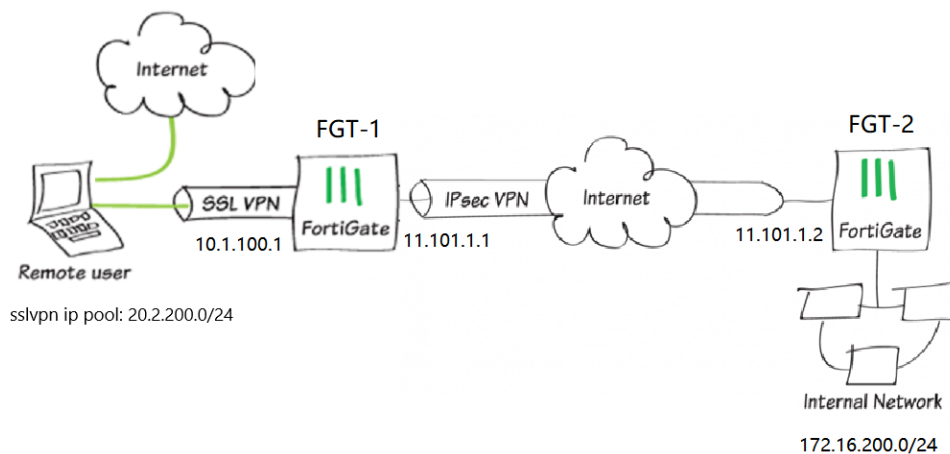
## SSL VPN to IPsec VPN

This is a sample configuration of site-to-site IPsec VPN that allows access to the remote endpoint via SSL VPN.

This example uses a pre-existing user group, a tunnel mode SSL VPN with split tunneling, and a route-based IPsec VPN between two FortiGates. All sessions must start from the SSL VPN interface.

If you want sessions to start from the FGT\_2 subnet, you need more policies. Also, if the remote subnet is beyond FGT\_2 (if there are multiple hops), you need to include the SSL VPN subnet in those routers as well.

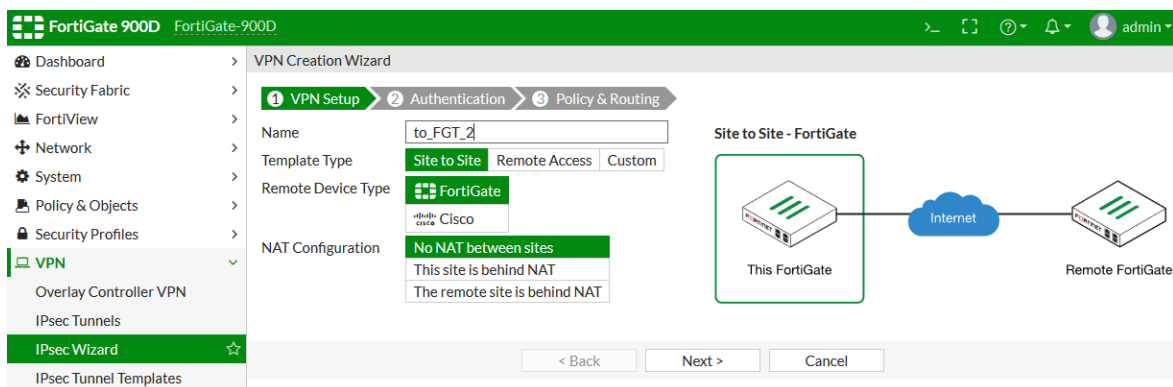
## Sample topology



## Sample configuration

To configure the site-to-site IPsec VPN on FGT\_1:

1. Go to *VPN > IPsec Wizard*.
2. In the *VPN Setup* pane:
  - a. Specify the VPN connection *Name* as *to\_FGT\_2*.
  - b. Select *Site to Site*.
  - c. Click *Next*.



3. In the *Authentication* pane:
  - a. Enter the *IP Address* to the Internet-facing interface.
  - b. For *Authentication Method*, click *Pre-shared Key* and enter the *Pre-shared Key*.

c. Click **Next**.

FortiGate 900D FortiGate-900D

VPN Creation Wizard

VPN Setup 2 Authentication 3 Policy & Routing

Remote Device: IP Address 11.101.1.2

Outgoing Interface: port12 (Detected via routing lookup)

Authentication Method: Pre-shared Key

Pre-shared Key: [Masked]

aa: Site to Site - FortiGate

This FortiGate --- Internet --- Remote FortiGate

< Back Next > Cancel

4. In the **Policy & Routing** pane:

- Set the **Local Interface** to the internal interface.
- Set the **Local Subnets** to include the internal and SSL VPN subnets for FGT\_1.
- Set **Remote Subnets** to include the internal subnet for FGT\_2.
- Click **Create**.

FortiGate 900D FortiGate-900D

VPN Creation Wizard

VPN Setup 2 Authentication 3 Policy & Routing

Local Interface: port10

Local Subnets: 10.1.100.0/24, 20.2.200.0/24

Remote Subnets: 172.16.200.0/24

Internet Access: None (Share Local, Use Remote)

to\_FGT\_2: Site to Site - FortiGate

This FortiGate --- Internet --- Remote FortiGate

< Back Create Cancel

A confirmation screen shows a summary of the configuration including the firewall address groups for both the local and remote subnets, static routes, and security policies.

FortiGate 900D FortiGate-900D

VPN Creation Wizard

VPN Setup 2 Authentication 3 Policy & Routing

The VPN has been set up

Summary of Created Objects

Phase 1 Interface	to_FGT_2	
Local Address Group	to_FGT_2_local	Edit
Remote Address Group	to_FGT_2_remote	Edit
Phase 2 Interface	to_FGT_2	
Static Route	2	Edit
Blackhole Route	3	Edit
Local to Remote Policy	vpn_to_FGT_2_local (1)	Edit
Remote to Local Policy	vpn_to_FGT_2_remote (2)	Edit

Add Another Show Tunnel List

### To configure SSL VPN settings:

1. Go to *VPN > SSL-VPN Settings*.
2. Set *Listen on Interface(s)* to *wan1*.
3. To avoid port conflicts, set *Listen on Port* to *10443*.
4. For *Restrict Access*, select *Allow access from any host*.
5. In the *Tunnel Mode Client Settings* section, select *Specify custom IP ranges* and include the SSL VPN subnet range created by the *IPsec Wizard*.
6. In the *Authentication/Portal Mapping* section, add the *VPN user group* to the *tunnel-access Portal*. Set *All Other Users/Groups* to the *web-access Portal*.

**FortiGate 900D** FortiGate-900D

Dashboard > Security Fabric > FortiView > Network > System > Policy & Objects > Security Profiles > **VPN**

Overlay Controller VPN  
IPsec Tunnels  
IPsec Wizard  
IPsec Tunnel Templates  
SSL-VPN Portals  
**SSL-VPN Settings**  
VPN Location Map  
User & Device > WiFi & Switch Controller > Log & Report > Monitor >

### SSL-VPN Settings

**Connection Settings**

Listen on Interface(s): port10

Listen on Port: 10443

Web mode access will be listening at <https://10.1.100.1:10443>

Redirect HTTP to SSL-VPN: ☐

Restrict Access: **Allow access from any host** | Limit access to specific hosts

Idle Logout: ☒

Inactive For: 300 Seconds

Server Certificate: Fortinet\_Factory

You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and upload it for use.  
[Click here to learn more](#)

Require Client Certificate: ☐

**Tunnel Mode Client Settings**

Address Range: Automatically assign addresses | **Specify** | Edit

IP Ranges: to\_FGT\_2\_local\_subnet\_2

DNS Server: Same as client system DNS | Specify

Specify WINS Servers: ☐

**Authentication/Portal Mapping**

+ Create New | Edit | Delete

Users/Groups	Portal
VPN user group	tunnel-access
All Other Users/Groups	web-access

Apply

7. Click *Apply*.

### To configure SSL VPN portal:

1. Go to *VPN > SSL-VPN Portals*.
2. Select *tunnel-access* and click *Edit*.
3. Turn on *Enable Split Tunneling* so that only traffic intended for the local or remote networks flow through FGT\_1 and follows corporate security profiles.
4. For *Routing Address*, add the local and remote IPsec VPN subnets created by the *IPsec Wizard*.

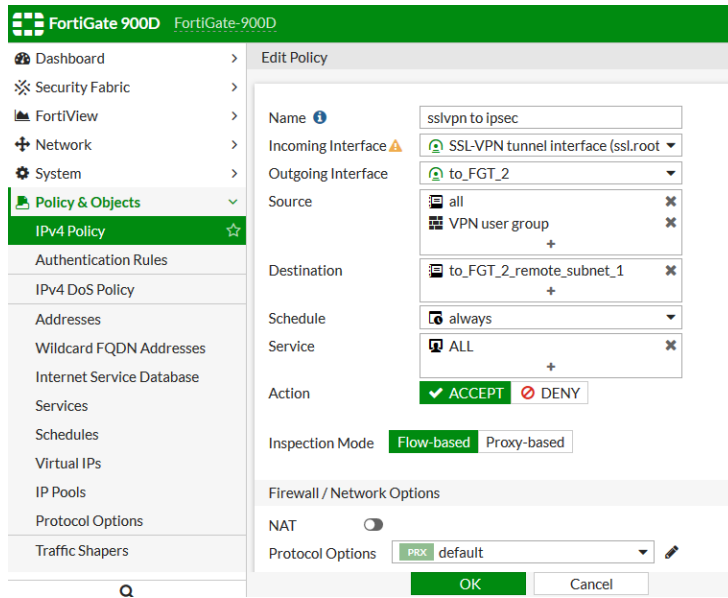
5. For *Source IP Pools*, add the SSL VPN subnet range created by the *IPsec Wizard*.

6. Click **OK**.

### To add policies to FGT\_1:

1. Go to *Policy & Objects* > *IPv4 Policy*.
2. Click *Create New* to create a policy that allows SSL VPN users access to the IPsec VPN tunnel.
3. For *Incoming Interface*, select *ssl.root*.
4. For *Outgoing Interface*, select the IPsec tunnel interface *to\_FGT\_2*.
5. Set the *Source* to *all* and the *VPN user group*.
6. Set *Destination* to the remote IPsec VPN subnet.
7. Specify the *Schedule*.
8. Set the *Service* to *ALL*.

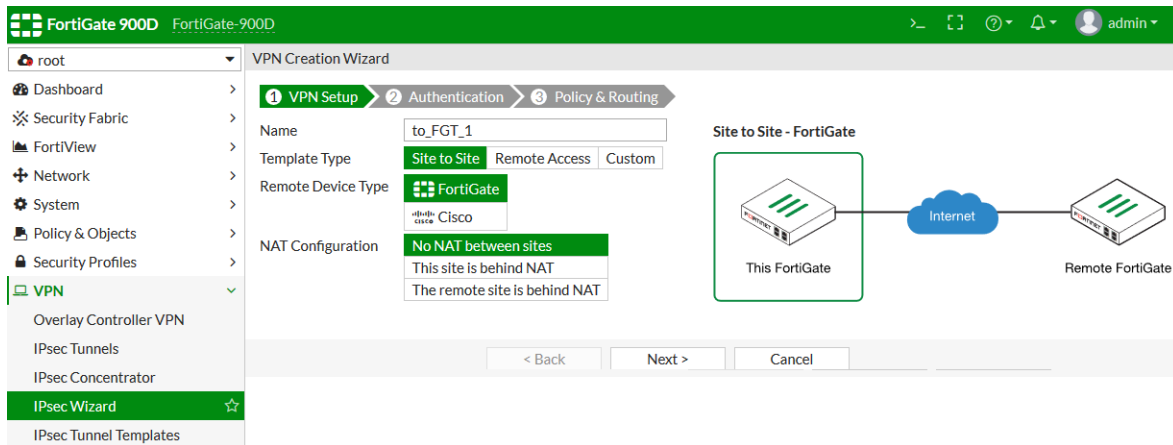
9. In the *Firewall/Network Options* section, disable *NAT*.



10. Click **OK**.

### To configure the site-to-site IPsec VPN on FGT\_2:

1. Go to *VPN > IPsec Wizard*.
2. In the *VPN Setup* pane:
  - a. Specify the VPN connection *Name* as *to\_FGT\_1*.
  - b. Select *Site to Site*.
  - c. Click *Next*.



3. In the *Authentication* pane:
  - a. Enter the *IP Address* to the Internet-facing interface.
  - b. For *Authentication Method*, click *Pre-shared Key* and enter the *Pre-shared Key* of the FGT\_1.



c. Click *Next*.

FortiGate 900D FortiGate-900D

VPN Creation Wizard

VPN Setup 2 Authentication 3 Policy & Routing

Remote Device IP Address Dynamic DNS

IP Address 11.101.1.1

Outgoing Interface port12 Change

Detected via routing lookup

Authentication Method Pre-shared Key Signature

Pre-shared Key

to\_FGT\_1: Site to Site - FortiGate

This FortiGate Remote FortiGate

< Back Next > Cancel

4. In the *Policy & Routing* pane:

- Set the *Local Interface* to the internal interface.
- Set the *Local Subnets* to include the internal and SSL VPN subnets for FGT\_2.
- Set *Remote Subnets* to include the internal subnet for FGT\_1.
- Click *Create*.

FortiGate 900D FortiGate-900D

VPN Creation Wizard

VPN Setup 2 Authentication 3 Policy & Routing

Local Interface port9

Local Subnets 172.16.200.0/24

Remote Subnets 10.1.100.0/24 20.2.200.0/24

Internet Access None Share Local Use Remote

to\_FGT\_1: Site to Site - FortiGate

This FortiGate Remote FortiGate

< Back Create Cancel

A confirmation screen shows a summary of the configuration including the firewall address groups for both the local and remote subnets, static routes, and security policies.

FortiGate 900D FortiGate-900D

VPN Creation Wizard

VPN Setup 2 Authentication 3 Policy & Routing

The VPN has been set up

Summary of Created Objects

Phase 1 Interface to\_FGT\_1

Local Address Group to\_FGT\_1\_local Edit

Remote Address Group to\_FGT\_1\_remote Edit

Phase 2 Interface to\_FGT\_1

Static Route 2 Edit

Blackhole Route 3 Edit

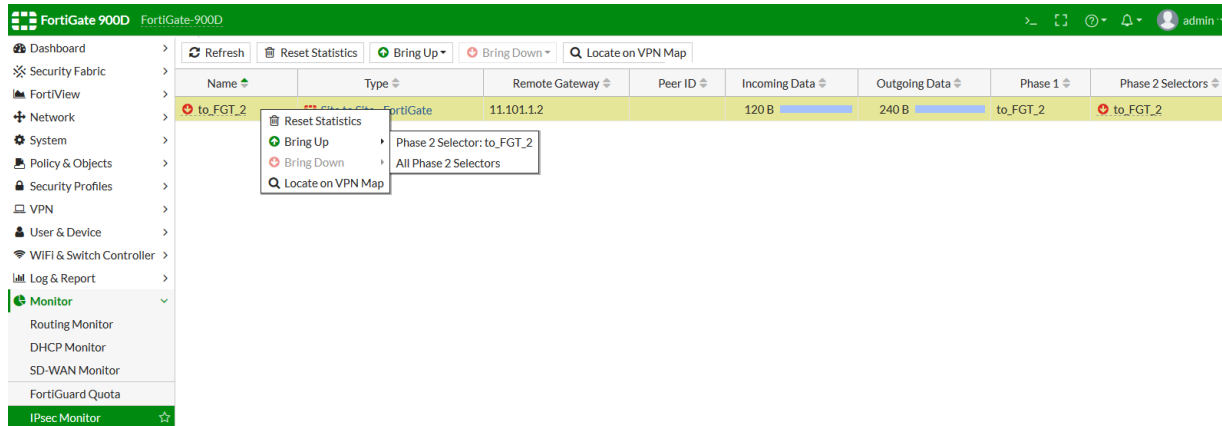
Local to Remote Policy vpn\_to\_FGT\_1\_local (1) Edit

Remote to Local Policy vpn\_to\_FGT\_1\_remote (2) Edit

Add Another Show Tunnel List

### To check the results:

1. Go to *Monitor > IPsec Monitor*.
2. Select the tunnel and click *Bring Up*.



3. Verify that the *Status* changes to *Up*.

Refresh

Reset Statistics

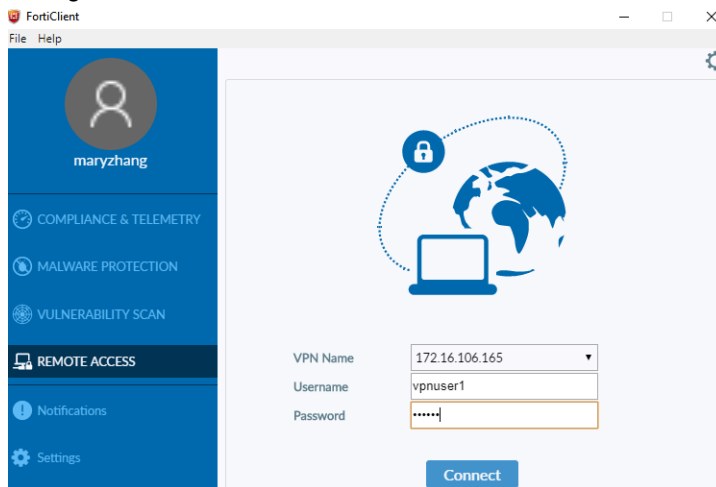
Bring Up

Bring Down

Locate on VPN Map

Name	Type	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
to_FGT_2	Site to Site - FortiGate	11.101.1.2		120 B	240 B	to_FGT_2	to_FGT_2

4. Configure the SSL VPN connection on the user's FortiClient and connect to the tunnel.



5. On the user's computer, use CLI to send a ping though the tunnel to the remote endpoint to confirm access.

```

C:\Users\maryzhang>ping 172.16.200.55

Pinging 172.16.200.55 with 32 bytes of data:
Reply from 172.16.200.55: bytes=32 time=2ms TTL=62
Reply from 172.16.200.55: bytes=32 time=1ms TTL=62
Reply from 172.16.200.55: bytes=32 time=1ms TTL=62
Reply from 172.16.200.55: bytes=32 time=1ms TTL=62

Ping statistics for 172.16.200.55:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\maryzhang>

```

6. Go to **Monitor > Routing Monitor** and verify that the routes for the IPsec and SSL VPNs are added.

FortiGate 900D FortiGate-900D

Static & Dynamic Policy

Type	Network	Gateway IP	Interfaces	Distance
Connected	10.1.100.0/24	0.0.0.0	port10	0
Connected	10.2.2.0/24	0.0.0.0	port11	0
Connected	10.6.30.0/24	0.0.0.0	mgmt1	0
Connected	11.101.1.0/24	0.0.0.0	port12	0
Static	172.16.200.0/24	0.0.0.0	to_FGT_2	10

7. Go to **Monitor > SSL-VPN Monitor** and verify user connectivity.

FortiGate 900D FortiGate-900D

SSL-VPN Monitor

Username	Last Login	Remote Host	Active Connections
vpnuser1	2019/08/12 11:30:32	10.1.100.254	Tunnel: 20.2.200.1

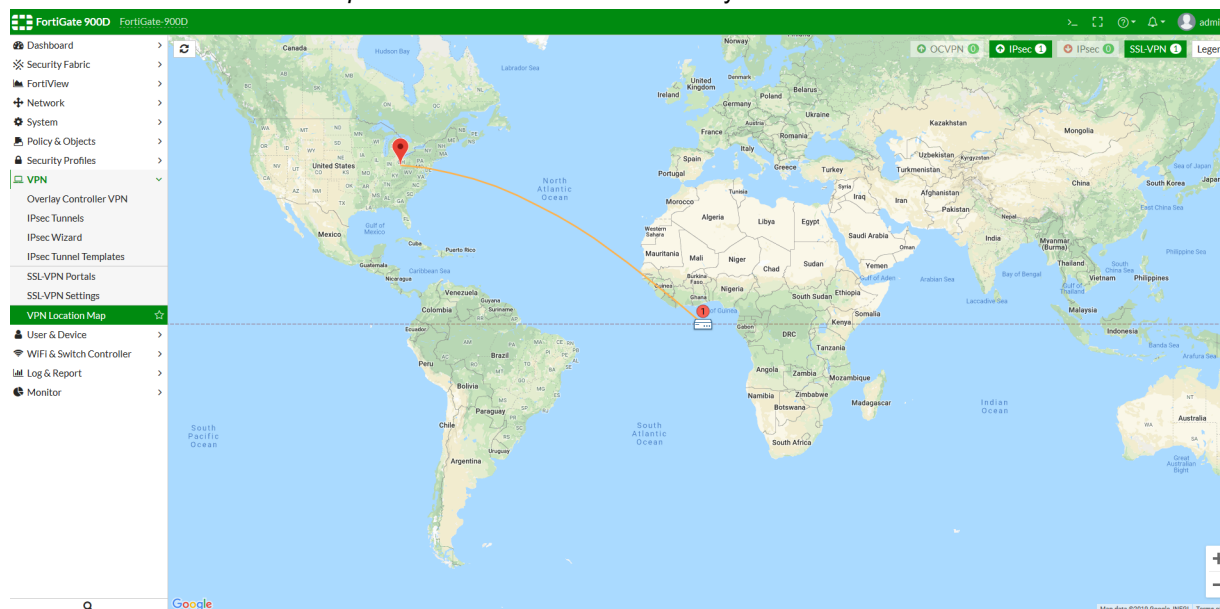
8. Go to **Log & Report > Events**, select **VPN Events** from the event type dropdown list, and view the IPsec and SSL tunnel statistics.

FortiGate 900D FortiGate-900D

VPN Events

Date/Time	Level	Action	Status	Message	VPN Tunnel
2019/08/12 11:44:45	Info	tunnel-up		SSL tunnel established	
2019/08/12 11:44:45	Info	ssl-new-con		SSL new connection	
2019/08/12 11:44:44	Info	tunnel-up		SSL tunnel established	
2019/08/12 11:44:44	Info	ssl-new-con		SSL new connection	
2019/08/12 11:44:44	Info	ssl-exit-error		SSL exit error	
2019/08/12 11:44:34	Info	ssl-new-con		SSL new connection	
2019/08/12 11:44:33	Info	tunnel-down		SSL tunnel shutdown	
2019/08/12 11:44:33	Info	tunnel-down		SSL tunnel shutdown	
2019/08/12 11:41:42	Info	negotiate	success	negotiate IPsec phase 2	to_FGT_2
2019/08/12 11:41:42	Info	negotiate	success	progress IPsec phase 2	to_FGT_2
2019/08/12 11:41:42	Info	phase2-up		IPsec phase 2 status change	to_FGT_2
2019/08/12 11:41:42	Info	install_sa		install IPsec SA	to_FGT_2
2019/08/12 11:41:42	Info	negotiate	success	progress IPsec phase 2	to_FGT_2
2019/08/12 11:40:33	Info	tunnel-stats		SSL tunnel statistics	
2019/08/12 11:40:07	Info	phase2-down		IPsec phase 2 status change	to_FGT_2
2019/08/12 11:40:07	Info	phase2-down		IPsec phase 2 status change	to_FGT_2
2019/08/12 11:35:55	Info	tunnel-stats		IPsec tunnel statistics	to_FGT_2
2019/08/12 11:30:33	Info	tunnel-up		SSL tunnel established	
2019/08/12 11:30:32	Info	ssl-new-con		SSL new connection	
2019/08/12 11:30:32	Info	tunnel-up		SSL tunnel established	
2019/08/12 11:30:32	Info	ssl-new-con		SSL new connection	
2019/08/12 11:30:32	Info	ssl-exit-error		SSL exit error	
2019/08/12 11:25:55	Info	tunnel-stats		IPsec tunnel statistics	to_FGT_2
2019/08/12 11:20:28	Info	negotiate	success	negotiate IPsec phase 2	to_FGT_2
2019/08/12 11:20:28	Info	negotiate	success	progress IPsec phase 2	to_FGT_2
2019/08/12 11:20:28	Info	negotiate	success	progress IPsec phase 2	to_FGT_2

9. Go to **VPN > VPN Location Map** and view VPN connection activity.



10. Go to **FortiView > Policies** and view policy usage.

Policy	Policy Type	Source Interface	Destination Interface	Bytes	Sessions	Bandwidth
sslvpn to ipsec (3)	IPv4	SSL-VPN tunnel interface (ssl.root)	to_FGT_2	52.44 kB	1	896 bps

## Troubleshooting

**To troubleshoot on FGT\_1, use the following CLI commands:**

```
diagnose debug reset
diagnose debug flow show function-name enable
diagnose debug flow show iprope enable
diagnose debug flow filter addr 172.16.200.55
diagnose debug flow filter proto 1
diagnose debug flow trace start 2
diagnose debug enable
```

**To troubleshoot using ping:**

1. Send a ping through the SSL VPN tunnel to 172.16.200.55 and analyze the output of the debug.
2. Disable the debug output with this command: `diagnose debug disable`.

If traffic is entering the correct VPN tunnel on FGT\_1, then run the same commands on FGT\_2 to check whether the traffic is reaching the correct tunnel. If it is reaching the correct tunnel, confirm that the SSL VPN tunnel range is configured in the remote side quick mode selectors.

**To troubleshoot using a sniffer command:**

```
diagnose sniff packet any "host 172.16.200.44 and icmp" 4
```

**To troubleshoot IPsec VPN issues, use the following commands on either FortiGate:**

```
diagnose debug reset
diagnose vpn ike gateway clear
diagnose debug application ike -1
diagnose debug enable
```

## SSL VPN protocols

The following topics provide information about SSL VPN protocols:

- [TLS 1.3 support on page 1479](#)
- [SMBv2 support on page 1480](#)

### TLS 1.3 support

#### SSL VPN

FortiOS supports TLS 1.3 for SSL VPN.



TLS 1.3 support requires IPS engine 4.205 or later and endpoints running FortiClient 6.2.0 or later.

---

**To establish a client SSL VPN connection with TLS 1.3 to the FortiGate:****1. Enable TLS 1.3 support using the CLI:**

```
config vpn ssl setting
 set ssl-max-proto-ver tls1-3
 set ssl-min-proto-ver tls1-3
end
```

**2. Configure the SSL VPN and firewall policy:**

- a. Configure the SSL VPN settings and firewall policy as needed.

**3. For Linux clients, ensure OpenSSL 1.1.1a is installed:**

- a. Run the following commands in the Linux client terminal:

```
root@PC1:~/tools# openssl
OpenSSL> version
```

If OpenSSL 1.1.1a is installed, the system displays a response like the following:

```
OpenSSL 1.1.1a 20 Nov 2018
```

**4. For Linux clients, use OpenSSL with the TLS 1.3 option to connect to SSL VPN:**

- a. Run the following command in the Linux client terminal:

```
#openssl s_client -connect 10.1.100.10:10443 -tls1_3
```

**5. Ensure the SSL VPN connection is established with TLS 1.3 using the CLI:**

```
diagnose debug application sslvpn -1
diagnose debug enable
```

The system displays a response like the following:

```
[207:root:ld]SSL established: TLSv1.3 TLS_AES_256_GCM_SHA384
```

## Deep inspection (flow-based)

FortiOS supports TLS 1.3 for policies that have the following security profiles applied:

- Web filter profile with flow-based inspection mode enabled.
- Deep inspection SSL/SSH inspection profile.

For example, when a client attempts to access a website that supports TLS 1.3, FortiOS sends the traffic to the IPS engine. The IPS engine then decodes TLS 1.3 and the client is able to access the website.

## SMBv2 support

On all FortiGate models, SMBv2 is enabled by default for SSL VPN. Client PCs can access the SMBv2 server using SSL VPN web-only mode.

### To configure SMBv2:

1. Set the minimum and maximum SMB versions.

```
config vpn ssl web portal
 edit portal-name
 set smb-min-version smbv2
 set smb-max-version smbv3
 next
end
```

2. Configure SSL VPN and firewall policies as usual.
3. Connect to the SSL VPN web portal and create an SMB bookmark for the SMBv2 server.
4. Click the bookmark to connect to the SMBv2 server.
5. On the FortiGate, use package capture to verify that SMBv2 works:

8	-440785802.3...	172.16.200.10	172.16.200.44	SMB2	252 Negotiate Protocol Request
9	-440785802.3...	172.16.200.44	172.16.200.10	SMB2	338 Negotiate Protocol Response

## SSL VPN troubleshooting

The following topics provide information about SSL VPN troubleshooting:

- [Debug commands on page 1480](#)
- [Troubleshooting common scenarios on page 1481](#)

## Debug commands

### SSL VPN debug command

Use the following diagnose commands to identify SSL VPN issues. These commands enable debugging of SSL VPN with a debug level of -1 for detailed results.

```
diagnose debug application sslvpn -1
diagnose debug enable
```

The CLI displays debug output similar to the following:

```
FGT60C3G10002814 # [282:root]SSL state:before/accept initialization (172.20.120.12)
[282:root]SSL state:SSLv3 read client hello A (172.20.120.12)
[282:root]SSL state:SSLv3 write server hello A (172.20.120.12)
[282:root]SSL state:SSLv3 write change cipher spec A (172.20.120.12)
[282:root]SSL state:SSLv3 write finished B (172.20.120.12)
[282:root]SSL state:SSLv3 flush data (172.20.120.12)
[282:root]SSL state:SSLv3 read finished A:system lib(172.20.120.12)
[282:root]SSL state:SSLv3 read finished A (172.20.120.12)
[282:root]SSL state:SSL negotiation finished successfully (172.20.120.12)
[282:root]SSL established: DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
```

### To disable the debug:

```
diagnose debug disable
diagnose debug reset
```

## Remote user authentication debug command

Use the following diagnose commands to identify remote user authentication issues.

```
diagnose debug application fnbamd -1
diagnose debug reset
```

## Troubleshooting common scenarios

### To troubleshoot getting no response from the SSL VPN URL:

1. Go to *VPN > SSL-VPN Settings*.
  - a. Check the SSL VPN port assignment.
  - b. Check the *Restrict Access* setting to ensure the host you are connecting from is allowed.
2. Go to *Policy > IPv4 Policy* or *Policy > IPv6 policy*.
  - a. Check that the policy for SSL VPN traffic is configured correctly.
  - b. Check the URL you are attempting to connect to. It should follow this pattern:
 

```
https://<FortiGate IP>:<Port>
```
  - c. Check that you are using the correct port number in the URL. Ensure FortiGate is reachable from the computer.
 

```
ping <FortiGate IP>
```
  - d. Check the browser has *TLS 1.1*, *TLS 1.2*, and *TLS 1.3* enabled.

### To troubleshoot FortiGate connection issues:

1. Check the Release Notes to ensure that the FortiClient version is compatible with your version of FortiOS.
2. FortiClient uses IE security setting, In IE *Internet options > Advanced > Security*, check that *Use TLS 1.1* and *Use TLS 1.2* are enabled.
3. Check that SSL VPN *ip-pools* has free IPs to sign out. The default *ip-poolsSSLVPN\_TUNNEL\_ADDR1* has 10 IP addresses.
4. Export and check FortiClient debug logs.
  - a. Go to *File > Settings*.
  - b. In the *Logging* section, enable *Export logs*.

- c. Set the *Log Level* to *Debug* and select *Clear logs*.
- d. Try to connect to the VPN.
- e. When you get a connection error, select *Export logs*.

#### To troubleshoot SSL VPN hanging or disconnecting at 98%:

1. A new SSL VPN driver was added to FortiClient 5.6.0 and later to resolve SSL VPN connection issues. If your FortiOS version is compatible, upgrade to use one of these versions.
2. Latency or poor network connectivity can cause the login timeout on the FortiGate. In FortiOS 5.6.0 and later, use the following commands to allow a user to increase the SSL VPN login timeout setting.

```
config vpn ssl settings
 set login-timeout 180 (default is 30)
 set dtls-hello-timeout 60 (default is 10)
end
```

#### To troubleshoot tunnel mode connections shutting down after a few seconds:

This might occur if there are multiple interfaces connected to the Internet, for example, SD-WAN. This can cause the session to become “dirty”. To allow multiple interfaces to connect, use the following CLI commands.

If you are using a FortiOS 6.0.1 or later:

```
config system interface
 edit <name>
 set preserve-session-route enable
 next
end
```

If you are using a FortiOS 6.0.0 or earlier:

```
config vpn ssl settings
 set route-source-interface enable
end
```

#### To troubleshoot users being assigned to the wrong IP range:

1. Go to *VPN > SSL-VPN Portals* and *VPN > SSL-VPN Settings* and ensure the same *IP Pool* is used in both places. Using the same *IP Pool* prevents conflicts. If there is a conflict, the portal settings are used.

#### To troubleshoot slow SSL VPN throughput:

Many factors can contribute to slow throughput.

This recommendation tries to improve throughput by using the FortiOS Datagram Transport Layer Security (DTLS) tunnel option, available in FortiOS 5.4 and above.

DTLS allows SSL VPN to encrypt traffic using TLS and uses UDP as the transport layer instead of TCP. This avoids retransmission problems that can occur with TCP-in-TCP.

FortiClient 5.4.0 to 5.4.3 uses DTLS by default. FortiClient 5.4.4 and later uses normal TLS, regardless of the DTLS setting on the FortiGate.

To use DTLS with FortiClient:

1. Go to *File > Settings* and enable *Preferred DTLS Tunnel*.

To enable DTLS tunnel on FortiGate, use the following CLI commands:



```
config vpn ssl settings
 set dtls-tunnel enable
end
```

# User & Device

In *User & Device*, you can control network access for different users and devices in your network. FortiGate authentication controls system access by user group. By assigning individual users to the appropriate user groups you can control each user's access to network resources. You can define local users and peer users on the FortiGate unit. You can also define user accounts on remote authentication servers and connect them to FortiOS.

You can control network access for different device types in your network by doing the following:

- Identifying and monitoring the types of devices connecting to your network
- Using MAC address based access control to allow or deny individual devices
- Using Telemetry data received from FortiClient endpoints to construct a policy to deny access to endpoints with known vulnerabilities or to quarantine compromised endpoints

The following sections provide information about users and devices:

- [Endpoint control and compliance on page 1484](#)
- [User Definition on page 1494](#)
- [User Groups on page 1495](#)
- [Guest Management on page 1502](#)
- [Device Inventory on page 1506](#)
- [LDAP Servers on page 1510](#)
- [RADIUS Servers on page 1520](#)
- [TACACS+ Servers on page 1531](#)
- [Authentication Settings on page 1532](#)
- [FortiTokens on page 1534](#)
- [Configuring the maximum log in attempts and lockout period on page 1556](#)
- [Creating a PKI/peer user on page 1557](#)
- [Configuring firewall authentication on page 1557](#)

## Endpoint control and compliance

### Per-policy disclaimer messages

FortiOS supports a customizable captive portal to direct users to install or enable required software.

Per-policy custom disclaimers in each VDOM are supported. For example, you may want to configure three firewall policies, each of which matches traffic from endpoints with different FortiClient statuses:

Endpoint status	FortiOS behavior
Endpoint does not have FortiClient installed.	Traffic matches a firewall policy that displays an in-browser warning to install FortiClient from the provided link.

Endpoint status	FortiOS behavior
Endpoint has FortiClient installed, registered to EMS, and connected to the FortiGate.	Traffic matches a dynamic firewall policy which allows the endpoint to reach its destination via this policy.
Endpoint is deregistered from EMS and disconnected from the FortiGate.	Traffic matches another dynamic firewall policy that displays warning to register FortiClient to EMS.

### To enable per-policy disclaimer messages:

```
config user setting
 set auth-cert "Fortinet_Factory"
 set per-policy-disclaimer enable
end
```

### To configure per-policy disclaimers in the GUI:

1. Ensure the per-policy disclaimer messages option is enabled.
2. Go to *Policy & Objects > IPv4 Policy*.
3. Edit the policy that applies when an endpoint does not have FortiClient installed.
4. Under *Disclaimer Options*, enable *Display Disclaimer*.
5. Enable *Customize Messages* then click *Edit Disclaimer Message*. The default disclaimer message is shown.
6. Edit the message to warn users to install FortiClient, and provide the FortiClient download link.

7. Click **Save**.
8. Repeat the above steps for each policy that requires a custom disclaimer message.

### To configure per-policy disclaimers in the CLI:

```
config firewall policy
 edit 1
 set name "111"
 set uuid c3ad8da0-bd7c-51e8-c0da-fe9053bf35ae
```

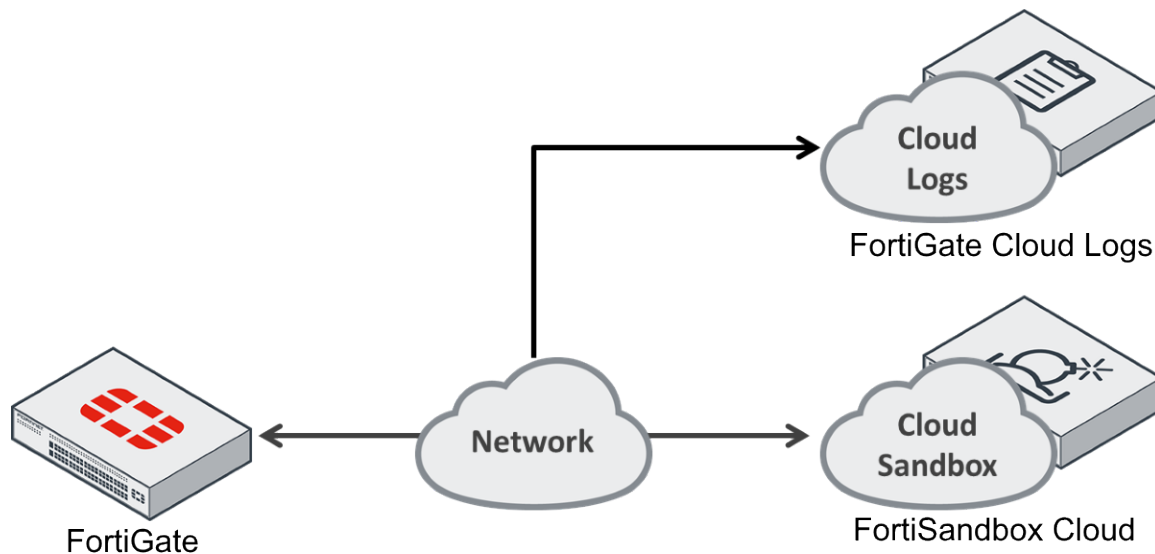
```
set srcintf "port12"
set dstintf "port11"
set srcaddr "all"
set dstaddr "pc155_address"
set action accept
set schedule "always"
set service "ALL"
set wso disable
set groups "ems_03_group"
set disclaimer enable
set replacemsg-override-group "test"
set nat enable
next
edit 4
set name "44"
set uuid 686ea2ca-348d-51e9-9dca-b2b4b4aabbbe2
set srcintf "port12"
set dstintf "port11"
set srcaddr "all"
set dstaddr "pc5-address"
set action accept
set schedule "always"
set service "ALL"
set wso disable
set groups "ems_03_group"
set disclaimer enable
set replacemsg-override-group "test2"
set nat enable
next
edit 6
set name "66"
set uuid f1034e52-36d5-51e9-fbae-da21922ccd10
set srcintf "port12"
set dstintf "port11"
set srcaddr "all"
set dstaddr "all"
set status disable
set schedule "always"
set service "ALL"
set logtraffic all
set fsso disable
set block-notification enable
set replacemsg-override-group "endpoint-override"
next
end
```

## Compliance

### FortiSandbox Cloud region selection

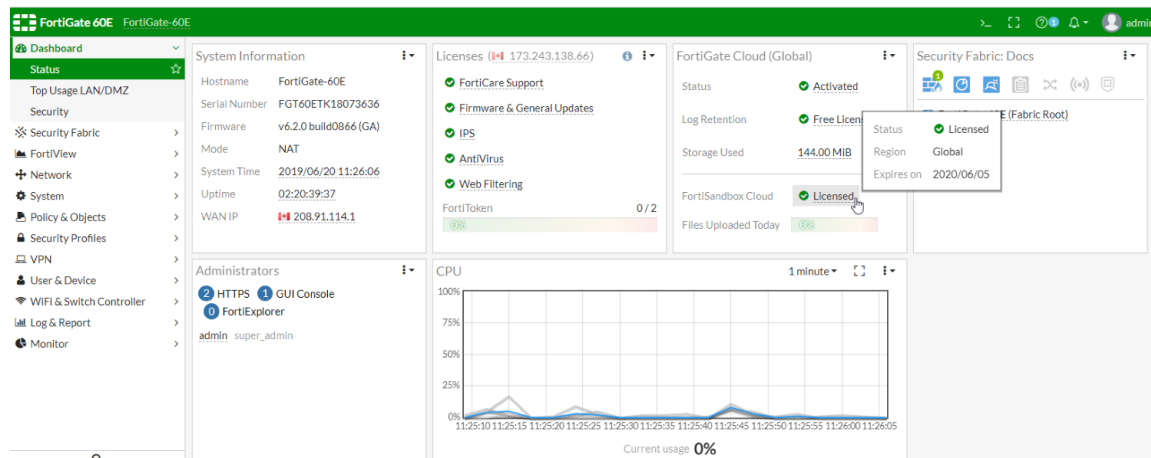
In FortiOS, FortiSandbox Cloud services are decoupled from the FortiGate Cloud license. This allows you to specify a FortiSandbox Cloud region and take advantage of FortiSandbox features without a FortiGate Cloud account.

The following topology demonstrates how FortiGate Cloud Logs and FortiSandbox Cloud are separated in FortiOS:



### To view the FortiGate Cloud Log and FortiSandbox licenses:

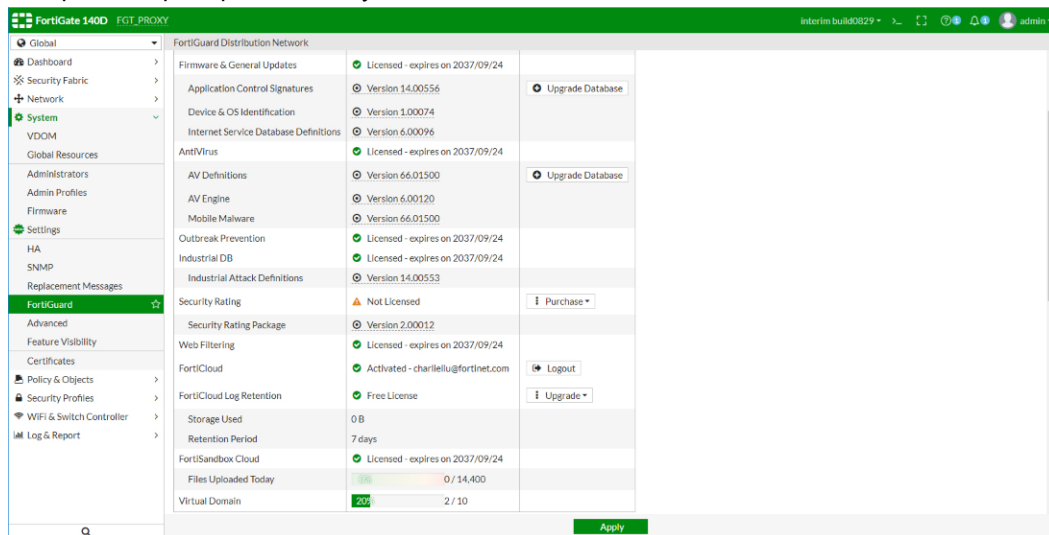
1. Go to *Dashboard > Status*.
2. The *FortiGate Cloud* widget shows separate license statuses for *Log Retention* and *FortiSandbox Cloud*. In the following example, the FortiGate Cloud account is using a free license, and FortiSandbox Cloud is using a paid license:



### To obtain a FortiSandbox Cloud license:

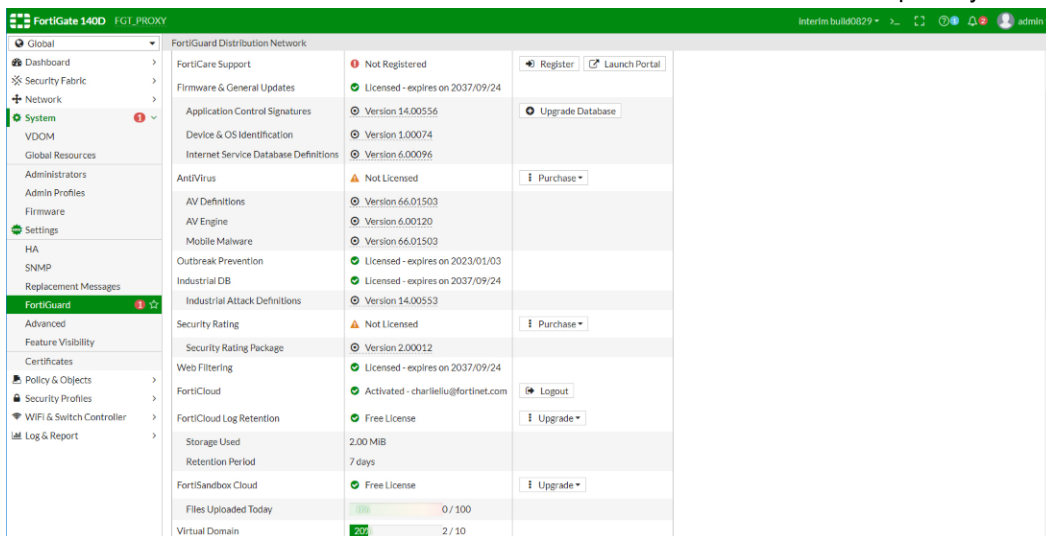
1. Go to *System > FortiGuard*.
2. Under *License Information > FortiSandbox Cloud*, click *Activate*.

### 3. Complete the prompts to obtain your license.



The FortiSandbox Cloud license is linked to your antivirus license, so they will expire at the same time.

- If the FortiGate is not registered with a paid antivirus license, the FortiGate will use the free FortiGate Cloud license. This license limits the FortiGate to 100 FortiSandbox Cloud submissions per day.



### To set the FortiSandbox Cloud region in the GUI:

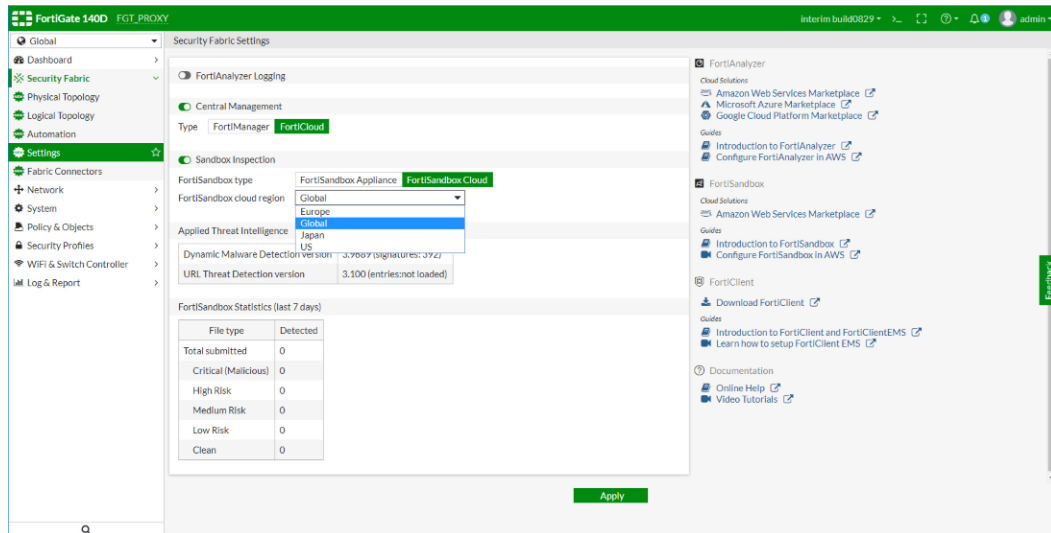
- Go to **Security Fabric > Settings**.
- In the **Sandbox Inspection** section, click **FortiSandbox Cloud**.
- Select a region from the **FortiSandbox cloud region** dropdown.

The following regions are available:

- Europe
- Global

- Japan
- US

#### 4. Click *Apply*.



#### To set the FortiSandbox Cloud region in the CLI:

```
FGT_PROXY (global) # execute forticloud-sandbox region
0 Europe
1 Global
2 Japan
3 US
Please select cloud sandbox region[0-3]:3
Cloud sandbox region is selected: US
```

The separation of the FortiGate Cloud Log and FortiSandbox services are visible in the following example:

```
FGT_PROXY (global) # diagnose test application forticldd 3
Debug zone info:
Domain:FortiCloud ReleaseQA Global - 172.16.95.16
Home log server: 172.16.95.93:514
Alt log server: 172.16.95.27:514
Active Server IP: 172.16.95.93
Active Server status: up
Log quota: 102400MB
Log used: 0MB
Daily volume: 20480MB
fams archive pause: 0
APTContract : 1
APT server: 172.16.102.52:514
APT Altserver: 172.16.102.51:514
Active APTServer IP: 172.16.102.52
Active APTServer status: up
```

## FortiGate VM unique certificate

To safeguard against certificate compromise, FortiGate VM and FortiAnalyzer VM use the same deployment model as FortiManager VM where the license file contains a unique certificate tied to the serial number of the virtual device.

A hardware appliance usually comes with a BIOS certificate with a unique serial number that identifies the hardware appliance. This built-in BIOS certificate is different from a firmware certificate. A firmware certificate is distributed in all appliances with the same firmware version.

Using a BIOS certificate with a built-in serial number provides a high trust level for the other side in X.509 authentication.

Since a VM appliance has no BIOS certificate, a signed VM license can provide an equivalent of a BIOS certificate. The VM license assigns a serial number in the BIOS equivalent certificate. This gives the certificate an abstract access ability, which is similar to a BIOS certificate with the same high trust level.



This feature is only supported in new, registered VM licenses.

## Sample configurations

Depending on the firmware version and VM license, the common name (CN) on the certificate will be configured differently.

### To view validated certificates:

1. Go to *System > Certificates*.
2. Double-click on a VM certificate. There are two VM certificates:
  - *Fortinet\_Factory*
  - *Fortinet\_Factory\_Backup*

The *Certificate Detail Information* window displays.

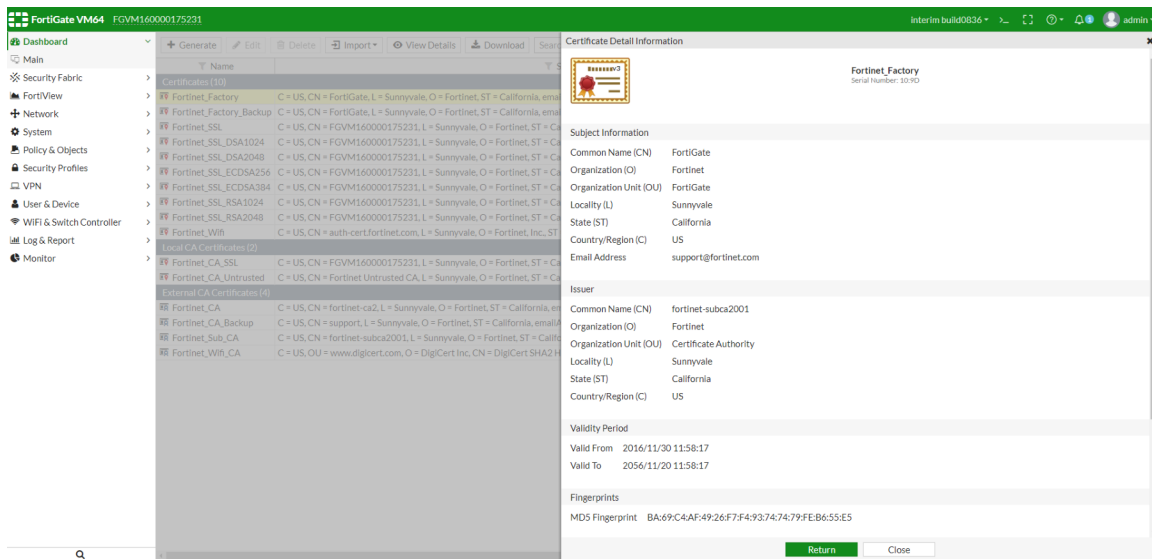
- If you are using new firmware (6.2.0 and later) with a new VM license, the CN becomes the FortiGate VM serial number.

The screenshot shows the FortiGate VM64 interface with the 'Certificates' section selected in the left sidebar. The main area displays a list of certificates. The 'Fortinet\_Factory' certificate is highlighted, and its details are shown in the 'Certificate Detail Information' window on the right.

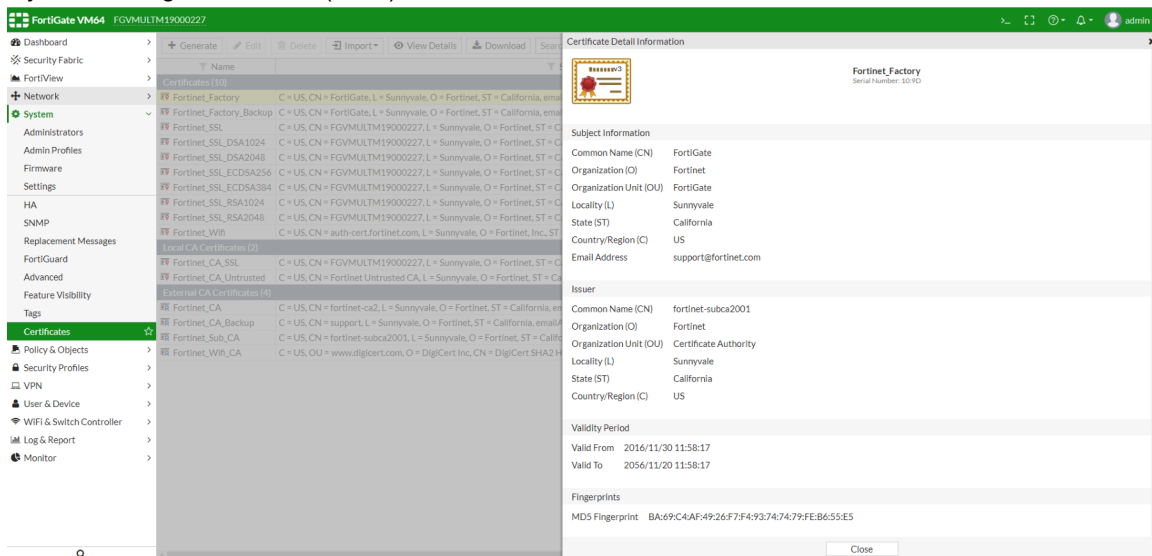
Section	Field	Value
Subject Information	Common Name (CN)	FGVMULTM19000227
	Organization (O)	Fortinet
	Organization Unit (OU)	FortiGate
	Locality (L)	Sunnyvale
	State (ST)	California
Country/Region (C)	US	
	Email Address	support@fortinet.com
Issuer	Common Name (CN)	fortinet-subca2001
	Organization (O)	Fortinet
	Organization Unit (OU)	Certificate Authority
	Locality (L)	Sunnyvale
	State (ST)	California
Country/Region (C)	US	
	Validity Period	
	Valid From	2019/03/01 15:40:54
	Valid To	2056/01/18 19:14:07
Fingerprints	MD5 Fingerprint	00:5E:9B:FE:5E:C5:E2:62:F2:EC:F1:3F:B1:E7:06:FC
	Extension	

- If you are using new firmware (6.2.0) with an old VM license, the CN remains as *FortiGate*. It does not change to the VM serial number.





- If you are using old firmware (6.0.2) with a new VM license, the CN remains as *FortiGate*.

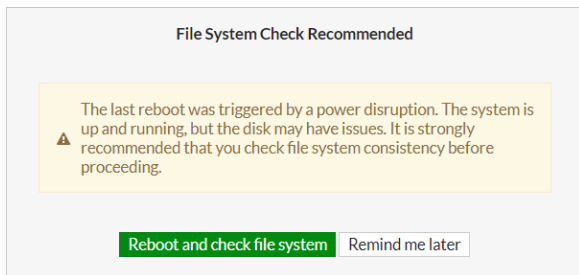


## Running a file system check automatically

There is an option in FortiOS to enable automatic file system checks if the FortiGate shuts down ungracefully.

By default, the automatic file system check is disabled. When an administrator logs in after an ungraceful shutdown, a warning message appears advising them to manually run a file system check.

GUI warning:



### CLI warning:

WARNING: File System Check Recommended! Unsafe reboot may have caused inconsistency in disk drive.

It is strongly recommended that you check file system consistency before proceeding. Please run 'execute disk scan 17'

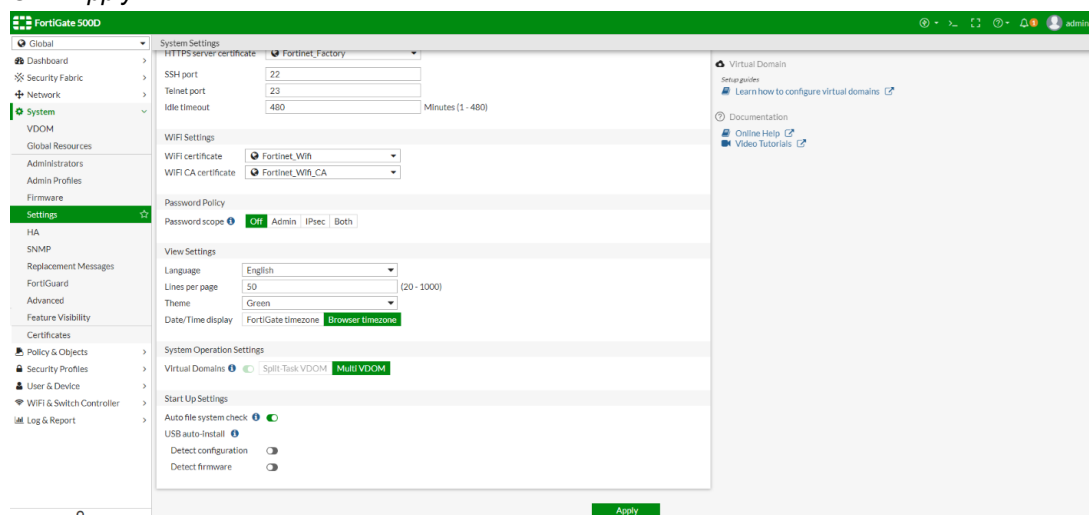
Note: The device will reboot and scan during startup. This may take up to an hour

### Enabling automatic file system checks

You can enable automatic file system checks in both the GUI and CLI.

#### To enable automatic file system checks in the GUI:

1. Go to *System > Settings*.
2. In the *Start Up Settings* section, enable *Auto file system check*.
3. Click *Apply*.



#### To enable automatic file system checks using the CLI:

```
config system global
 set autorun-log-fsck enable
end
```

## FortiGuard distribution of updated Apple certificates

Push notifications for iPhone (for the purpose of two-factor authentication) require a TLS server certificate to authenticate to Apple. As this certificate is only valid for one year, a service extension allows FortiGuard to distribute updated TLS server certificates to FortiGate when needed.

FortiGuard update service updates local Apple push notification TLS server certificates when the local certificate is expired. FortiGuard update service also reinstalls certificates when the certificates are lost.

You can verify that the feature is working on the FortiGate by using the CLI shell.

### To verify certificate updates:

1. Using FortiOS CLI shell, verify that all certificates are installed:

```
/data/etc/apns # ls -al
drwxr-xr-x 2 0 0 Tue Jan 15 08:42:39 2019 1024 .
drwxr-xr-x 12 0 0 Tue Jan 15 08:45:00 2019 2048 ..
-rw-r--r-- 1 0 0 Sat Jan 12 00:06:30 2019 2377 apn-dev-cert.pem
-rw-r--r-- 1 0 0 Sat Jan 12 00:06:30 2019 1859 apn-dev-key.pem
-rw-r--r-- 1 0 0 Sat Jan 12 00:06:30 2019 8964 apn-dis-cert.pem
-rw-r--r-- 1 0 0 Sat Jan 12 00:06:30 2019 4482 apn-dis-key.pem
```

2. Rename all current Apple certificates.

Apple push notification no longer works after you rename the certificates.

```
/data/etc/apns # mv apn-dis-cert.pem apn-dis-cert.pem.save
/data/etc/apns # mv apn-dev-key.pem apn-dev-key.pem.save
/data/etc/apns # mv apn-dev-cert.pem apn-dev-cert.pem.save
/data/etc/apns # mv apn-dis-key.pem apn-dis-key.pem.save
/data/etc/apns # ls -al
drwxr-xr-x 2 0 0 Tue Jan 15 08:51:15 2019 1024 .
drwxr-xr-x 12 0 0 Tue Jan 15 08:45:00 2019 2048 ..
-rw-r--r-- 1 0 0 Sat Jan 12 00:06:30 2019 2377 apn-dev-cert.pem.save
-rw-r--r-- 1 0 0 Sat Jan 12 00:06:30 2019 1859 apn-dev-key.pem.save
-rw-r--r-- 1 0 0 Sat Jan 12 00:06:30 2019 8964 apn-dis-cert.pem.save
-rw-r--r-- 1 0 0 Sat Jan 12 00:06:30 2019 4482 apn-dis-key.pem.save
```

3. Run a FortiGuard update, and verify that all certificates are installed again:

```
/data/etc/apns # ls -al
drwxr-xr-x 2 0 0 Tue Jan 15 08:56:20 2019 1024 .
drwxr-xr-x 12 0 0 Tue Jan 15 08:56:15 2019 2048 ..
-rw-r--r-- 1 0 0 Sat Jan 12 00:06:30 2019 2377 apn-dev-cert.pem.save
-rw-r--r-- 1 0 0 Sat Jan 12 00:06:30 2019 1859 apn-dev-key.pem.save
-rw-r--r-- 1 0 0 Tue Jan 15 08:56:20 2019 2167 apn-dis-cert.pem <-- downloaded
from FortiGuard
-rw-r--r-- 1 0 0 Sat Jan 12 00:06:30 2019 8964 apn-dis-cert.pem.save
-rw-r--r-- 1 0 0 Tue Jan 15 08:56:20 2019 1704 apn-dis-key.pem <-- downloaded
from FortiGuard
-rw-r--r-- 1 0 0 Sat Jan 12 00:06:30 2019 4482 apn-dis-key.pem.save
-rw-r--r-- 1 0 0 Tue Jan 15 08:56:20 2019 41 apn-version.dat <-- downloaded
from FortiGuard
/data/etc/apns #
```

## User Definition

The following topics provide information about user definition:

- [User types on page 1494](#)
- [Removing a user on page 1494](#)

### User types

You can configure FortiOS users in FortiOS or on an external authentication server. The following summarizes user account types and authentication in FortiOS:

User type	Authentication
Local	Username and password must match a user account stored in FortiOS. Authentication by FortiOS security policy.
Remote	Username and password must match a user account stored in FortiOS and on the remote authentication server. FortiOS supports LDAP, RADIUS, and TACACS+ servers.
Authentication server	A FortiOS user group can include user accounts or groups that exist on a remote authentication server.
FSSO	Microsoft Windows or Novell network users can use their network credentials to access resources through FortiOS. You can control access using FSSO user groups that contain Windows or Novell user groups as members.
PKI/peer	Digital certificate holder who authenticates using a client certificate. No password is required unless two-factor authentication is enabled.
IM	FortiOS does not authenticate IM users. FortiOS allows or blocks each IM user from accessing IM protocols. A global policy for each IM protocol governs unknown users' access to these protocols.
Guest	Guest user accounts are temporary. The account expires after a selected period of time. See <a href="#">Guest Management on page 1502</a> .

### Removing a user

When a user account is no longer in use, you should delete it. If any configuration objects, such as a user group, reference the user account, you must remove the references before deleting the user.

#### To remove references to a user:

1. Go to *User & Device > User Definition*.
2. If the value in the *Ref.* column is not 0, click it.
3. FortiOS displays a list of object references to the user. Use this information to remove these references.

**To remove a user using the GUI:**

1. Go to *User & Device > User Definition*.
2. Select the desired user.
3. Click *Delete*, then *OK*.

**To remove a user using the CLI:**

```
config user local
 delete exampleuser
end
```

## User Groups

A user group is a list of users. Security policies and some VPN configurations only allow access to specified user groups. This restricted access enforces role-based access control (RBAC) to your organization's network and resources. Users must be in a group and that group must be part of the security policy.

In most cases, FortiOS authenticates a user by requesting their username and password. FortiOS checks local user accounts first. Then, if it does not find a match, FortiOS checks the RADIUS, LDAP, and TACACS+ servers that belong to the user group. Authentication succeeds when FortiOS finds a matching username and password. If the user belongs to multiple groups on a server, FortiOS matches those groups as well.



FortiOS does not allow username overlap between RADIUS, LDAP, and TACACS+ servers.

---

## Configuring POP3 authentication

FortiOS can authenticate users who have accounts on POP3 or POP3s email servers.

**To configure POP3 authentication:**

```
config user pop3
 edit pop3_server1
 set server pop3.fortinet.com
 set secure starttls
 set port 110
 next
end
```

**To configure a POP3 user group:**

A user group can list up to six POP3 servers as members.

```
config user group
 edit pop3_grp
 set member pop3_server1
 next
```

end

## Dynamic policies - FortiClient EMS

The FortiClient EMS FSSO connector allows objects to be defined in FortiOS that map to tags and groups on EMS. EMS dynamically updates these endpoint groups when host compliance or other events occur, causing FortiOS to dynamically adjust its security policies based on the group definitions.

EMS supports creating compliance verification rules based on various criteria. When a FortiClient endpoint registers to EMS, EMS dynamically groups them based on these rules. FortiOS can receive the dynamic endpoint groups from EMS as tags via the FSSO protocol using an FSSO agent that supports SSL and imports trusted certificates.

After FortiOS pulls the tags from EMS, they can be used as members in user groups that can have dynamic firewall policies applied to them. When an event occurs, EMS sends an update to FortiOS, and the dynamic policies are updated.

The following instructions assume EMS is installed, configured, and has endpoints connected. For information on configuring EMS, see the [FortiClient EMS Administration Guide](#).

The following steps provide an example of configuring a dynamic policy:

1. [Add a compliance verification rule in EMS on page 1496](#)
2. [Configure an EMS FSSO agent on page 1497](#)
3. [Configure user groups on page 1498](#)
4. [Create a dynamic firewall policy on page 1499](#)

### Add a compliance verification rule in EMS

This example creates a compliance verification rule that applies to endpoints that have Windows 10 installed.

For more information see [Compliance verification](#) in the [FortiClient EMS Administration Guide](#).

#### To create a compliance verification rule in EMS:

1. In EMS, go to *Compliance Verification > Compliance Verification Rules*.
2. Click *Add*.
3. In the *Name* field, enter the desired rule name.  
EMS uses the tag name to dynamically group endpoints, not the rule name configured in this field.
4. Turn *Status* on to enable the rule.
5. For *Type*, select *Windows*, *Mac*, or *Linux*. This affects what rule types are available. In this example, *Windows* is selected.
6. From the *Rule* dropdown list, select the rule type and configure the related options. Ensure you click the + button after entering each criterion.  
In this example, *OS Version* is selected from the *Rule* dropdown list, and *Windows 10* is selected from the *OS Version* dropdown list.
7. Under *Assign to*, select *All*.
8. In the *Tag endpoint as* dropdown list, select an existing tag or enter a new tag. In this example, a new tag, WIN10\_EMS134, is created. EMS uses this tag to dynamically group together endpoints that satisfy the rule, as well as any other rules that are configured to use this tag.

**Add New Rule**

Name: Win 10

Status: ☒

Type: Windows (selected), Mac, Linux

Rule: OS Version

OS Version: Windows 10

Assign to: All

Tag endpoint as: WIN10\_EMS134

Save Cancel

9. Click **Save**.
10. Go to *Compliance Verification > Host Tag Monitor*. All endpoints that have Windows 10 installed are shown grouped by the WIN10\_EMS134 tag.

## Configure an EMS FSSO agent

In this example, the FSSO agent name is EMS\_FSSO\_connector, and the EMS server is located at 172.18.64.7.

### To configure the EMS FSSO agent in FortiOS in the GUI:

1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New*.
3. In the SSO/Identity section, click *Fortinet Single Sign-On Agent*.

**FortiGate 3100D FGT\_ECA**

**New Fabric Connector**

SSO/Identity

Fortinet Single Sign-On Agent

Connector Settings

Name: EMS\_FSSO\_connector

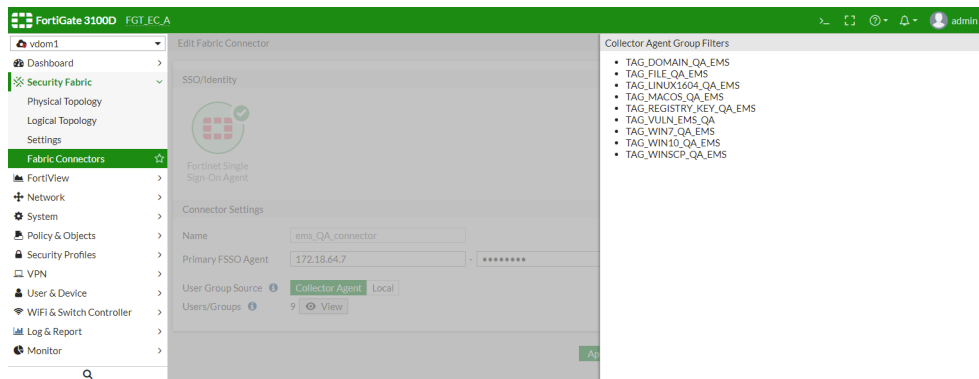
Primary FSSO Agent: 172.18.64.7

User Group Source: Collector Agent (Local)

Users/Groups: 0

Apply & Refresh OK Cancel

4. Fill in the *Name*, and *Primary FSSO Agent* server IP address or name and *Password*.
5. Set the *User Group Source* to *Collector Agent*.  
User groups will be pushed to the FortiGate from the collector agent. Click *Apply & Refresh* to fetch group filters from the collector agent.



6. Click **OK**.

### To configure the EMS FSSO agent in FortiOS in the CLI:

```
config user fsso
 edit "ems_QA_connector"
 set server "172.18.64.7"
 set password *****
 set type fortiems
 set ssl enable
 next
end
```

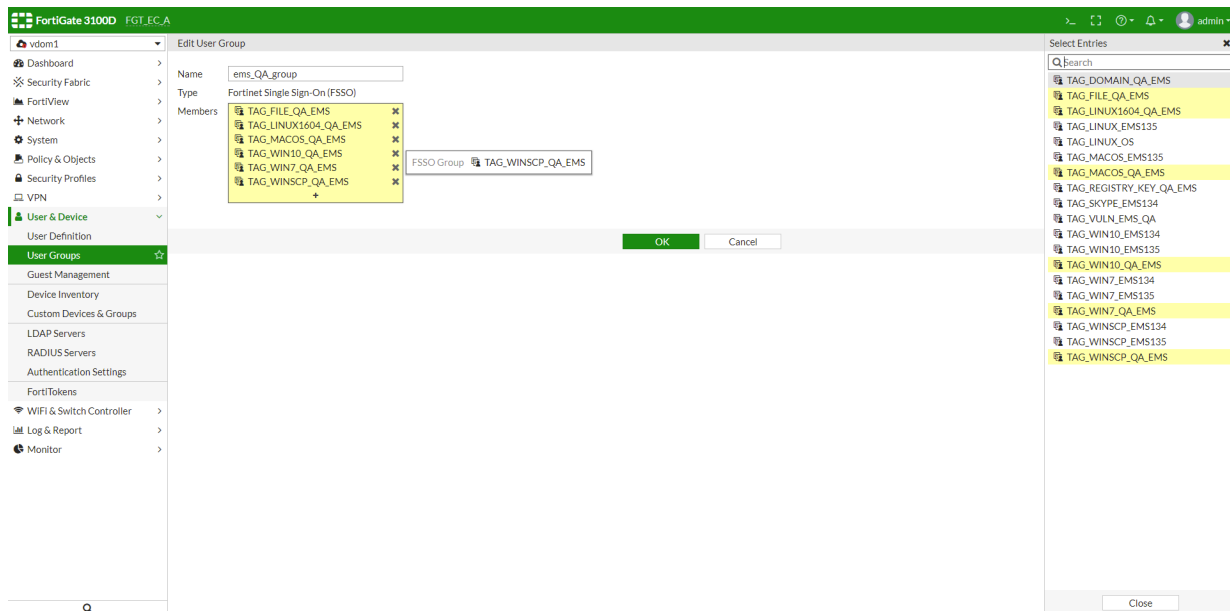
## Configure user groups

In this example, the user group is named `ems_QA_group`, and includes six dynamic endpoint groups that were pulled from EMS as members.

### To configure a user group based on EMS tags in the GUI:

1. Go to *User & Device > User Groups*.
2. Click *Create New*.
3. In the *Name* field, enter `ems_QA_group`.
4. For *Type*, select *Fortinet Single Sign-On (FSSO)*.
5. In the *Members* field, click **+**. The *Select Entries* pane appears. The dynamic endpoint groups pulled from EMS have names that begin with `TAG_`, followed by the tag name in EMS.
6. Select the desired dynamic endpoint groups. Endpoints that currently belong to these groups in EMS will be members of this FortiOS user group.





7. Click **OK**.

### To configure a user group based on EMS tags in the CLI:

```
config user group
 edit "ems_QA_group"
 set group-type fsso-service
 set authtimeout 0
 set http-digest-realm ''
 set member "TAG_FILE_QA_EMS" "TAG_LINUX1604_QA_EMS" "TAG_MACOS_QA_EMS" "TAG_WIN10_QA_EMS" "TAG_WIN7_QA_EMS" "TAG_WINSXP_QA_EMS"
 next
end
```

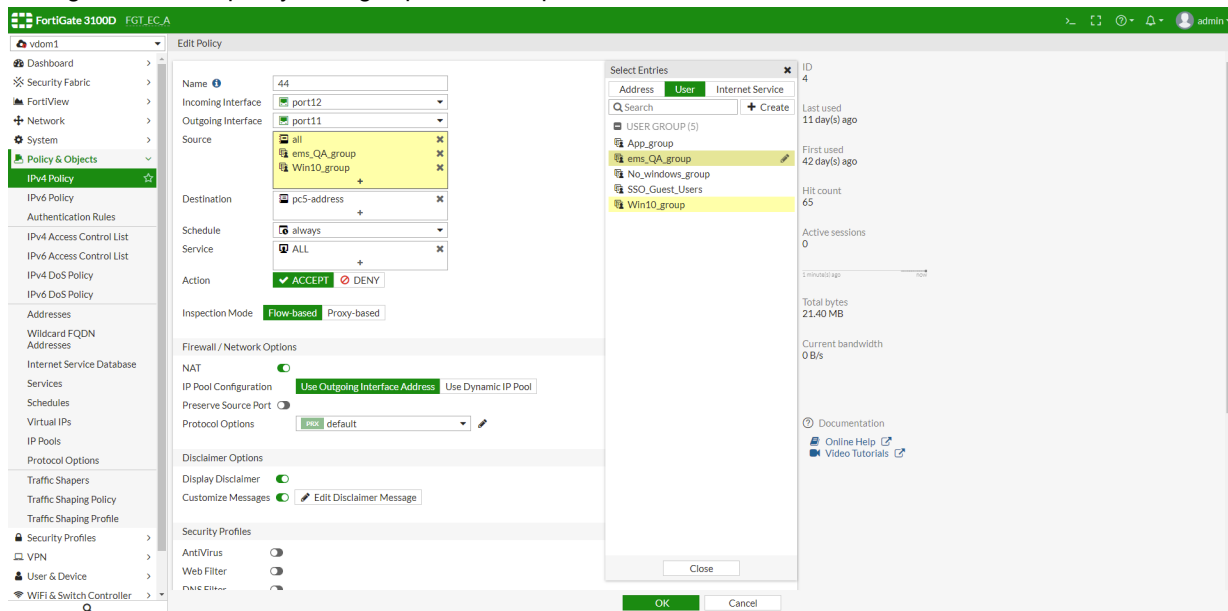
## Create a dynamic firewall policy

You can create a dynamic firewall policy for the user group. This example shows how to create an IPv4 policy for the user group.

### To create a dynamic firewall policy for the user group in the GUI:

1. Go to *Policy & Objects > IPv4 Policy*.
2. Click *Create New*.
3. In the *Source* field, click +. The *Select Entries* pane opens.
  - a. On the *User* tab, select the *ems\_QA\_group* group.
  - b. Click *Close*.

#### 4. Configure the other policy settings options as required.



#### 5. Click OK.

#### 6. Go to *Policy & Objects > IPv4 Policy* to ensure the policy was created and applied to the desired user group. FortiOS will update this policy when it receives updates from EMS.

### To create a dynamic firewall policy for the user group in the CLI:

```
config firewall policy
 edit 4
 set name 44
 set srcintf port12
 set dstintf port11
 set srcaddr "all" "ems_QA_group" "Win10_group"
 set dstaddr pc5-address
 set action accept
 set schedule always
 set service ALL
 next
end
```

## Diagnostics

To list endpoint records, use the following CLI command:

```
diagnose endpoint record-list
Record #1:
 IP_Address = 10.1.100.120(3)
 MAC_Address = 00:0c:29:36:4e:61
 Host MAC_Address = 00:0c:29:36:4e:61
 MAC list = 00-0c-29-36-4e-57;00-0c-29-36-4e-61;
 VDOM = vdom1
 EMS serial number: FCTEMS3688727941
 Quarantined: no
 Online status: online
```

```
On-net status: on-net
FortiClient connection route: Direct
FortiClient communication interface index: 19
DHCP server:
Dirty_onnet_addr: yes
FortiClient version: 6.2.0
AVDB version: 67.558
FortiClient app signature version: 14.586
FortiClient vulnerability scan engine version: 2.28
FortiClient feature version status: 0
FortiClient UID: FA4AFAF6F92442E69DC7D67ABE64BDBA (0)
FortiClient KA interval dirty: 0
FortiClient Full KA interval dirty: 0
Auth_AD_groups:
Auth_group: ems_QA_group
Auth_user: FRANK
Host_Name: DESKTOP-FJEVH8U
OS_Version: Microsoft Windows 10 Professional Edition, 64-bit (build 17763)
Host_Description: AT/AT COMPATIBLE
Domain:
Last_Login_User: frank
Host_Model: VMware Virtual Platform
Host_Manufacturer: VMware, Inc.
CPU_Model: Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz
Memory_Size: 4096
Installed features: 375
Enabled features: 177
Last vul message received time: N/A
Last vul scanned time: N/A
Last vul statistic: critical=0, high=0, medium=0, low=0, info=0
Avatar source username: frank
Avatar source email:
Avatar source: Client Operating System
Phone number:

online records: 1; offline records: 0; quarantined records: 0
```

To list authenticated IPv4 users, use the following CLI command:

```
diagnose firewall auth list
2.2.2.1, JONATHANWONG
 type: fsso, id: 0, duration: 18955, idled: 18955
 server: ems_QA_connector
 packets: in 0 out 0, bytes: in 0 out 0
10.1.100.111, FRANK111
 type: fsso, id: 0, duration: 18955, idled: 18955
 server: ems_QA_connector
 packets: in 0 out 0, bytes: in 0 out 0
 group_id: 5
 group_name: ems_QA_group
10.1.100.120, FRANK
 type: fsso, id: 0, duration: 18955, idled: 4
 server: ems_QA_connector
 packets: in 10643 out 11379, bytes: in 6014568 out 3224342
 group_id: 5
 group_name: ems_QA_group
10.1.100.141, ADMINISTRATOR
 type: fsso, id: 0, duration: 18955, idled: 1
```

```
server: ems_QA_connector
packets: in 9669 out 10433, bytes: in 5043948 out 2823319
group_id: 5
group_name: ems_QA_group
...
...

----- 23 listed, 0 filtered -----

FGT_EC_A (vdom1) # diagnose debug authd fsso list
----FSSO logons----
IP: 2.2.2.1 User: JONATHANWONG Groups: 6B8028751BF3457BA172EE3795A2BDA8 Workstation:
VAN-201740-PC
IP: 10.1.100.111 User: FRANK111 Groups: ECF57781AE384D6A9A4D2D72CB5169C6+TAG_
LINUX1604_QA_EMS Workstation: FRANK111- VIRTUAL-MACHINE MemberOf: ems_QA_group
IP: 10.1.100.120 User: FRANK Groups: FA4AFAF6F92442E69DC7D67ABE64BDBA+TAG_WIN10_QA_EMS
Workstation: DESKTOP-FJEVH8U MemberOf: ems_QA_group
IP: 10.1.100.141 User: ADMINISTRATOR Groups: 6D21827915CE445F8A85F9E6BAA0C57A+TAG_
VULN_EMS_QA+TAG_WIN7_QA_EMS Workstation: LHWIN7A MemberOf: ems_QA_group
....
....

Total number of logons listed: 23, filtered: 0
----end of FSSO logons----
```

## Guest Management

### Configuring guest access

A visitor to your premises may need a user account on your network during their stay. If you are hosting a large event, such as a conference, you may need to create many temporary accounts for the attendees. You can create many guest accounts simultaneously using randomly generated user IDs and passwords to reduce your workload for these large events.

The following describes managing guest access:

1. Create one or more guest user groups. All members of a group have the same user ID type, password type, information fields used, and type and time of expiry.
2. Create guest accounts.
3. Use captive portal authentication and select the appropriate guest group.
4. The guest receives an email, SMS message, or printout containing their user ID and password from the FortiOS administrator.
5. The guest logs onto the network using the provided credentials.
6. After the configured expiry time, the credentials are no longer valid.

This configuration consists of the following steps:

1. [Add an SMS service.](#)
2. [Create a guest management administrator.](#)
3. [Create a guest user group.](#)
4. [Create guest user accounts.](#)

### To add an SMS service:

To send SMS notifications to guest users, add an email to SMS service to your FortiGate using the following commands:

```
config system sms-server
 edit <server-name>
 set mail-server <server-name>
 next
end
```

### To create a guest management administrator:

1. Go to *System > Administrators*.
2. Click *Create New > Administrator*.
3. Enable *Restrict admin to guest account provisioning only*.
4. For *Guest Group*, select the desired guest groups.

### To create a guest user group:

The guest group configuration determines the provided fields when you create a guest user account.

1. Go to *User & Device > User Groups*.
2. Click *Create New*.
3. For *Type*, select *Guest*.
4. If desired, enable *Batch Guest Account Creation*. When this is enabled, the following is true:
  - User IDs and passwords are auto-generated.
  - User accounts only have the *User ID*, *Password*, and *Expiration* fields. You can only edit the *Expiration* field. If the expiry time is a duration, such as eight hours, the countdown starts at initial login.
  - You can print the account information to provide to the guest. Guests do not receive email or SMS notifications.
5. For *User ID*, select one of the following:

Option	Description
Email	Guest's email address.
Auto Generated	FortiOS creates a random user ID for the guest.
Specify	The administrator assigns a user ID to the guest.

6. For *Password*, select one of the following:

Option	Description
Disable	No password.
Auto Generated	FortiOS creates a random password for the guest.
Specify	The administrator assigns a password to the guest.

7. For *Start Countdown*, select one of the following:

Option	Description
On Account Creation	FortiOS counts expiry time from time of account creation.

Option	Description
After First Login	FortiOS counts expiry time from the guest's first login.

8. For *Time*, configure the expiry time. You can change this for individual users.
9. Configure any other field as required, then click *OK*.

## Creating guest user accounts

### To create a guest user account:

1. Go to *User & Device > Guest Management*.
2. Select the desired guest group.
3. Click *Create New*.
4. Configure the guest as desired.
5. Click *OK*.

### To create multiple guest user accounts automatically:

1. Go to *User & Device > Guest Management*.
2. Select the desired guest group. This group must have *Batch Guest Account Creation* enabled.
3. Click *Create New > Multiple Users*.
4. Enter the *Number of Accounts*.
5. If desired, change the expiry.
6. Click *OK*.

## Retail environment guest access

Businesses such as coffee shops provide free Internet access for customers. In this scenario, you do not need to configure guest management, as customers can access the WiFi access point without login credentials.

However, consider that the business wants to contact customers with promotional offers to encourage future patronage. You can configure an email collection portal to collect customer email addresses for this purpose. You can configure a security policy to grant network access only to users who provide a valid email address. The first time a customer's device attempts WiFi connection, FortiOS requests an email address, which it validates. The customers' subsequent connections go directly to the Internet without interruption.

This configuration consists of the following steps:

1. [Creating an email collection portal on page 1504](#)
2. [Creating a security policy on page 1505](#)
3. [Checking for harvested emails on page 1505](#)

### Creating an email collection portal

The customer's first contact with your network is a captive portal that presents a webpage requesting an email address. When FortiOS has validated the email address, the customer's device MAC address is added to the Collected Emails device group.

This example modifies the `freewifi` WiFi interface to present an email collection captive portal.

**To create an email collection portal:**

```
config wireless-controller vap
 edit freewifi
 set security captive-portal
 set portal-type email-collect
 next
end
```

**Creating a security policy**

You must configure a security policy that allows traffic to flow from the WiFi SSID to the internet interface only for members of the Collected Emails device group. This policy must be listed first. Unknown devices are not members of the Collected Emails device group, so they do not match the policy.

**To create a security policy:**

```
config firewall policy
 edit 3
 set srcintf "freewifi"
 set dstintf "wan1"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set nat enable
 set email-collect enable
 next
end
```

**Checking for harvested emails****To check for harvested emails in the GUI:**

1. Go to *Dashboard > Users & Devices*.
2. Hover over the *Device Inventory* widget and click *Expand to Full Screen*.

**To check for harvested emails in the CLI:**

```
diagnose user device list
hosts
 vd 0 d8:d1:aa:aa:69:0f gen 35 req 30 redir 1 last 43634s 7-11_2-int
 ip 10.0.2.101 ip6 fe80::dad2:cbff:feab:610f
 type 2 'iPhone' src http c 1 gen 29
 os 'iPhone' version 'iOS 6.0.1' src http id 358 c 1
 email 'yo@yourdomain.com'
 vd 0 74:e1:bb:bb:69:f9 gen 36 req 20 redir 0 last 39369s 7-11_2-int
 ip 10.0.2.100 ip6 fe80::76e2:b6ff:fedd:69f9
 type 1 'iPad' src http c 1 gen 5
 os 'iPad' version 'iOS 6.0' src http id 293 c 1
 host 'Joes's-iPad' src dhcp
 email 'you@fortinet.com'
```

## Device Inventory

You can enable device detection to allow FortiOS to monitor your networks and gather information about devices operating on those networks, including:

- MAC address
- IP address
- Operating system
- Hostname
- Username
- When FortiOS detected the device and on which interface

You can enable device detection separately on each interface in *Network > Interfaces*. Device detection is intended for devices directly connected to your LAN ports. If enabled on a WAN port, device detection may be unable to determine the OS on some devices. You can enable active scanning on the interface to find hosts whose device types FortiOS cannot determine passively.

You can also manually add devices to Device Inventory to ensure that a device with multiple interfaces displays as a single device.

The following topics provide information about Device Inventory:

- [Device summary and filtering on page 1506](#)
- [Adding MAC-based addresses to devices on page 1508](#)

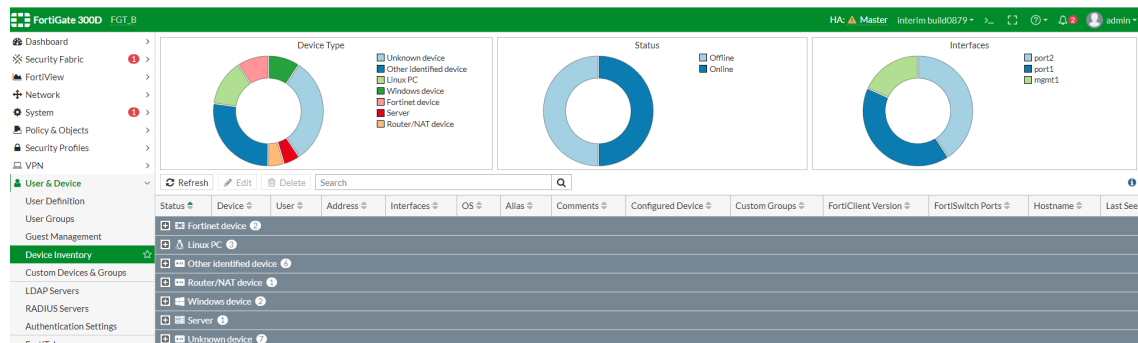
## Device summary and filtering

The *Device Inventory* pane contains three summary charts that provide an overview of the device type, status, and interfaces. You can use these clickable charts to simplify filtering among your devices.

**To view the device summary and apply a filter:**

1. Go to *User & Device > Device Inventory*.

The *Device Inventory* pane appears with the three charts:



2. Click one item in the chart (in the legend or chart area) to apply a filter. Once the filter is applied, the list of results displays beneath the charts.



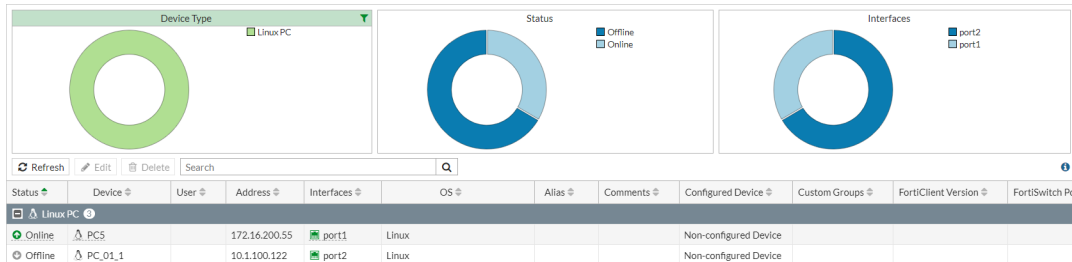


You can combine filters by clicking one item in another chart.

## Filter examples

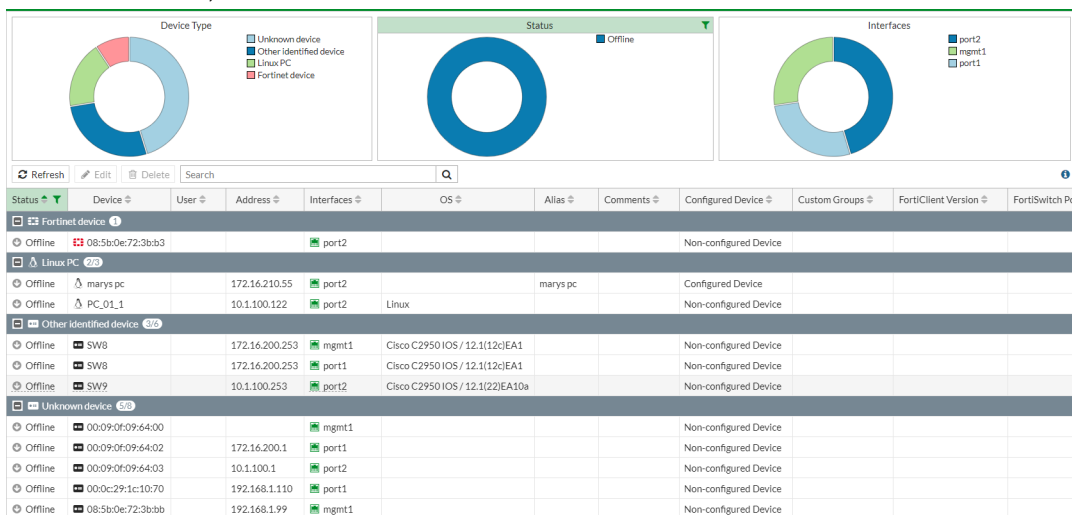
### To filter all Linux devices:

1. In the *Device Type* chart, click *Linux PC*.



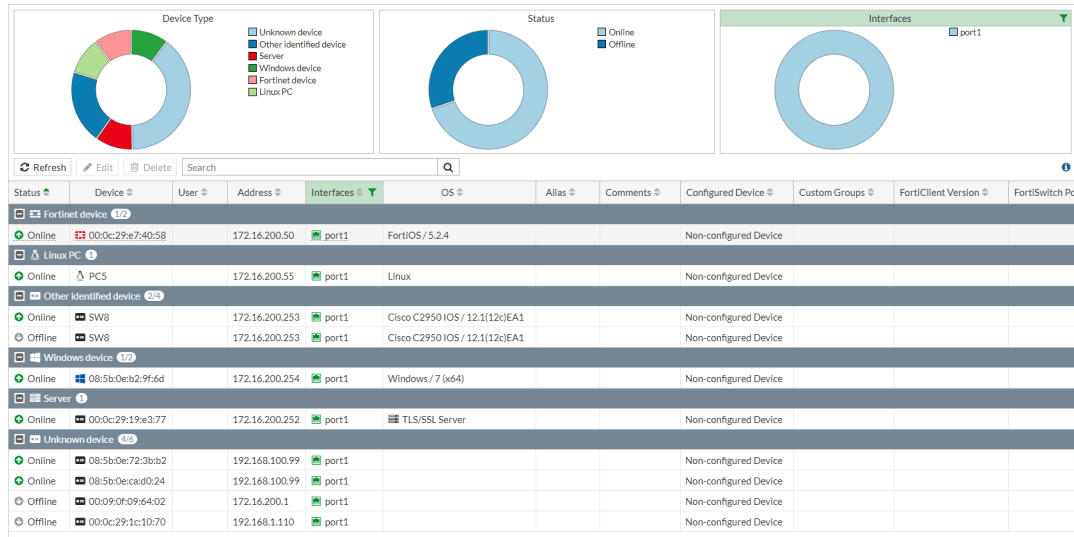
### To filter all offline devices:

1. In the *Status* chart, click *Offline*.



## To filter all devices discovered on port1:

1. In the *Interfaces* chart, click *port1*.



Click the filter icon in the top-right corner of the chart to remove the filter.

## Adding MAC-based addresses to devices

Assets detected by device detection appear in the *User & Device > Device Inventory* list. You can manage policies around devices by adding a new device object (MAC-based address) to a device. Once you add the MAC-based address, the device can be used in address groups or directly in policies.

## To add a MAC-based address to a device:

1. Go to *User & Device > Device Inventory*.
2. Right-click a device and select *Create Firewall Address > MAC Address*.

Status	Device	User	Address	Interfaces	Software OS	Device Family	Hardware Version
Online	uipg_dev_dev1@00:08:e3:ed:35:16		uipg_dev_dev1@00:08:e3:ed:35:16	port1	Other identified device		
Online	uipg_dev_dev2@00:0c:29:19:e3:77		uipg_dev_dev2@00:0c:29:19:e3:77	port1	Other identified device		
Online	uipg_dev_dev3@00:0c:29:a9:a8:93		172-16-200-55	port1	Other identified device		
Online	00:0c:29:73:36:00		00:0c:29:73:36:00	port2	Other identified device		
Online	00:0c:29:73:36:00		00:0c:29:73:36:00	port2	Other identified device		
Online	00:0c:29:73:36:00		00:0c:29:73:36:00	port1	Other identified device		
Online	00:13:80:c5:67:96		00:13:80:c5:67:96	port2	Other identified device		
Online	08:5b:0e:72:3fa2		08:5b:0e:72:3fa2	port1	Other identified device		
Online	08:5b:0e:b2:9f:6d		08:5b:0e:b2:9f:6d	port1	Other identified device		
Offline	00:09:0f:09:8f:06		00:09:0f:09:8f:06	port2	Other identified device		
Offline	00:0c:29:1c:10:66		00:0c:29:1c:10:66	port2	Other identified device		
Offline	00:0c:29:1c:10:70		00:0c:29:1c:10:70	port1	Other identified device		
Offline	00:0c:29:a8:23:4c		00:0c:29:a8:23:4c	port2	Other identified device		

3. In the *New Address* pane, enter an address name.

**New Address**

Category: Address IPv6 Address

Name: 00:0c:29:a7:40:58

Color: [Change]

Type: Device (MAC Address)

MAC Address Scope: Single Address Range

MAC Address: 00:0c:29:a7:40:58

Interface: port1

Show in Address List: [On]

Comments: Write a comment...

OK Cancel

4. Click **OK**. The MAC address icon is now displayed in the *Address* column for the device.

Status	Device	User	Address	Interfaces	Software OS	Device Family	Hardware Version
Online	upg_dev_dev1@00:08:e3:ed:35:16		upg_dev_dev1@00:08:e3:ed:35:16	port1	Other identified device		
Online	upg_dev_dev2@00:0c:29:19:a3:77		upg_dev_dev2@00:0c:29:19:a3:77	port1 port2	Other identified device		
Online	00:0c:29:e7:40:58		00:0c:29:e7:40:58	port1	Other identified device		
Online	00:13:80:c5:67:96		00:13:80:c5:67:96	port2	Other identified device		
Online	08:5b:0e:72:3f:a2		08:5b:0e:72:3f:a2	port1	Other identified device		
Online	08:5b:0e:b2:9f:6d		08:5b:0e:b2:9f:6d	port1	Other identified device		
Offline	upg_dev_dev3@00:0c:29:a9:a8:93		172-16-200-55 upg_dev_dev3@00:0c:29:a9:a8:93	port1	Other identified device		
Offline	00:09:0f:09:8f:06		00:09:0f:09:8f:06	port2	Other identified device		
Offline	00:0c:29:1c:10:66		00:0c:29:1c:10:66	port2	Other identified device		
Offline	00:0c:29:1c:10:70		00:0c:29:1c:10:70	port1	Other identified device		
Offline	00:0c:29:73:36:00		00:0c:29:73:36:00	port2	Other identified device		
Offline	00:0c:29:a9:a8:9d		00:0c:29:a9:a8:9d	port2	Other identified device		
Offline	00:0c:29:e8:23:4c		00:0c:29:e8:23:4c	port2	Other identified device		

## LDAP Servers

### FSSO polling connector agent installation

This topic gives an example of configuring a local FSSO agent on the FortiGate. The agent actively pools Windows Security Event log entries on Windows Domain Controller (DC) for user log in information. The FSSO user groups can then be used in a firewall policy.

This method does not require any additional software components, and all the configuration can be done on the FortiGate.

#### To configure a local FSSO agent on the FortiGate:

1. [Configure an LDAP server on the FortiGate on page 1510](#)
2. [Configure a local FSSO polling connector on page 1511](#)
3. [Add the FSSO groups to a policy on page 1513](#)

### Configure an LDAP server on the FortiGate

#### To configure an LDAP server on the FortiGate:

1. Go to *User & Device > LDAP Servers*.
2. Click *Create New*.

## 3. Fill in the required information:

The screenshot shows the 'Edit LDAP Server' configuration page in the FortiGate 4000 web interface. The left sidebar shows the 'User & Device' menu with 'LDAP Servers' selected. The main content area contains the following fields:

- Name: FORTINET-FSSO
- Server IP/Name: 10.1.100.131
- Server Port: 389
- Common Name Identifier: sAMAccountName
- Distinguished Name: dc=FORTINET-FSSO,dc=com
- Bind Type: Simple, Anonymous, Regular (selected)
- Username: cn=admin,dc=FORTINET-FSSO,dc=com
- Password: \*\*\*\*\*
- Secure Connection: ☒
- Connection status: Successful
- Test User Credentials: [button]
- OK [button] Cancel [button]

- *Common Name Identifier* must be changed from the default value because, in a Windows environment, sAMAccountName must be unique, and cn must not be unique.
- *Distinguished Name* is the location in the LDAP tree where the FortiGate will start searching for user and group objects.
- *Active Directory* requires authentication by default, so the *Bind Type* is *Regular*, and the user account log in information is entered in the requisite fields. Optionally, click *Test User Credentials* to ensure that the account has sufficient access rights.

## 4. Click OK.

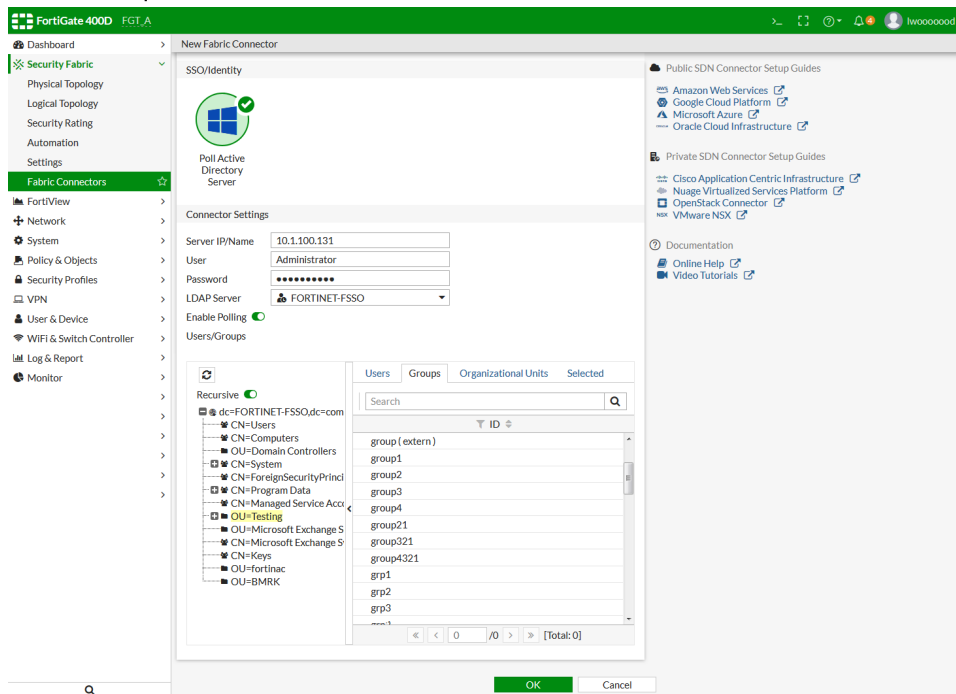
The FortiGate checks the connection, and updates the *Connection Status*. The connection must be successful before configuring the FSSO polling connector.

## Configure a local FSSO polling connector

### To configure a local FSSO polling connector:

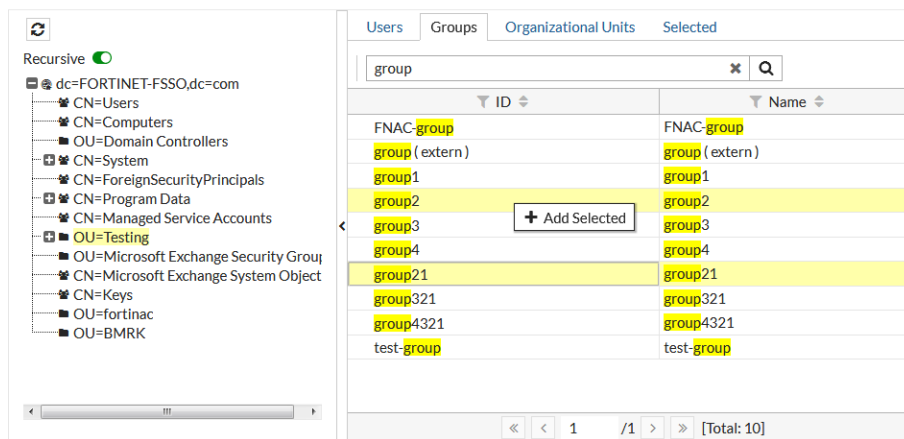
1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New*.
3. In the *SSO/Identity* section, select *Poll Active Directory Server*.

## 4. Fill in the required information.



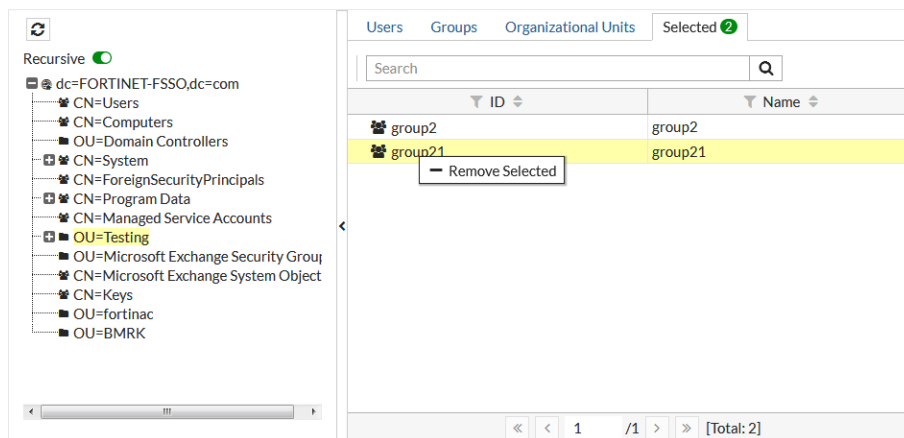
5. Select the just created LDAP server from the *LDAP Server* dropdown list. The structure of the LDAP tree will be shown in the *Users/Groups* section.
6. Go to the *Groups* tab.
7. Select the required groups, right click on them, and select *Add Selected*. Multiple groups can be selected at one time by holding the CTRL or SHIFT keys. The groups list can be filtered or searched to limit the number of groups that are displayed.

Users/Groups

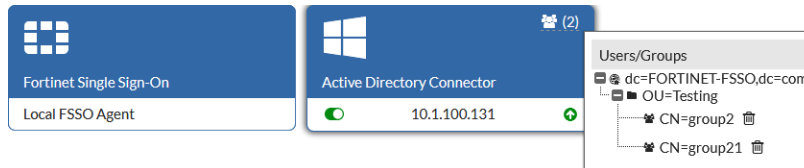


8. Go to the *Selected* tab and verify that all the required groups are listed. Unneeded groups can be removed by right clicking and selecting *Remove Selected*.

Users/Groups



9. Click OK.
10. Go back to *Security Fabric > Fabric Connectors*.
11. There should be two new connectors:



- The *Local FSSO Agent* is the backend process that is automatically created when the first FSSO polling connector is created.
- The *Active Directory Connector* is the front end connector that can be configured by FortiGate administrators.

To verify the configuration, hover the cursor over the top right corner of the connector; a popup window will show the currently selected groups. A successful connection is also shown by a green up arrow in the lower right corner of the connector.

If you need to get log in information from multiple DCs, then you must configure other Active Directory connectors for each additional DC to be monitored.

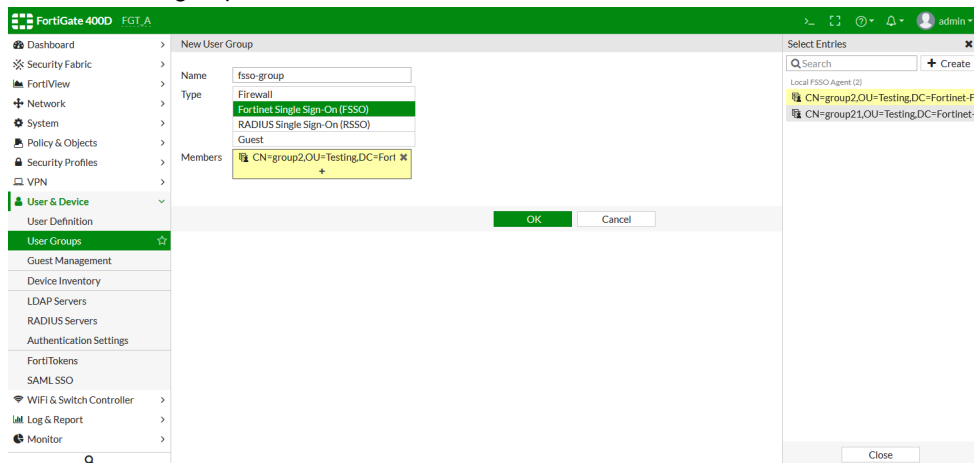
## Add the FSSO groups to a policy

FSSO groups can be used in a policy by either adding them to the policy directly, or by adding them to a local user group and then adding the group to a policy.

### To add the FSSO groups to a local user group:

1. Go to *User & Device > User Groups*.
2. Click *Create New*.
3. Enter a name for the group in the *Name* field.
4. Set the *Type* to *Fortinet Single Sign-On (FSSO)*.

## 5. Add the FSSO groups as members.

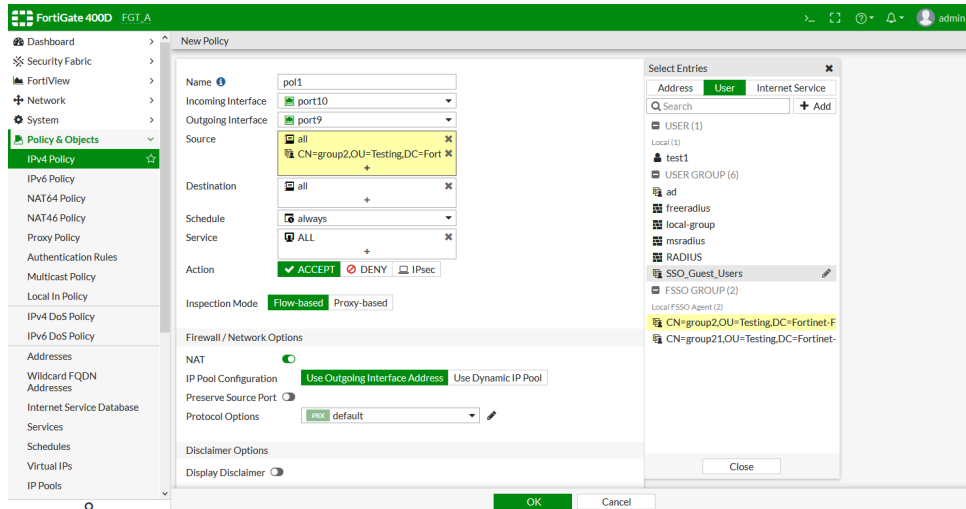


## 6. Click OK.

## 7. Add the local FSSO group to a policy.

To add the FSSO groups directly to a firewall policy:

1. Go to *Policy & Objects > IPv4 Policy*.
2. Click *Create New*.
3. Click in the *Source* field.
4. In the *Select Entries* pane, select the *User* tab.
5. Select the FSSO groups.



## 6. Configure the remaining settings as required.

## 7. Click OK.



## Troubleshooting

**If an authenticated AD user cannot access the internet or pass the firewall policy, verify the local FSSO user list:**

```
diagnose debug authd fsso list
----FSSO logons----
IP: 10.1.100.188 User: test2 Groups: CN=group2,OU=Testing,DC=Fortinet-FSSO,DC=COM
Workstation: MemberOf: CN=group2,OU=Testing,DC=Fortinet-FSSO,DC=COM
Total number of logons listed: 1, filtered: 0
----end of FSSO logons----
```

1. Check that the group in *MemberOf* is allowed by the policy.
2. If the expected AD user is not in list, but other users are, it means that either:
  - The FortiGate missed the log in event, which can happen if many users log in at the same time, or
  - The user's workstation is unable to connect to the DC, and is currently logged in with cached credentials, so there is no entry in the DC security event log.
3. If there are no users in the local FSSO user list:
  - a. Ensure that the local FSSO agent is working correctly:

```
diagnose debug enable
diagnose debug authd fsso server-status
```

Server Name	Connection Status	Version	Address
-----	-----	-----	-----
FGT_A (vdom1) # Local FSSO Agent	connected	FSAE server 1.1	127.0.0.1

The connection status must be connected.

- b. Verify the Active Directory connection status:

```
diagnose debug fsso-polling detail 1
AD Server Status (connected):
ID=1, name(10.1.100.131),ip=10.1.100.131,source(security),users(0)
port=auto username=Administrator
read log eof=1, latest logon timestamp: Fri Jul 26 10:36:20 2019
```

```
polling frequency: every 10 second(s) success(274), fail(0)
LDAP query: success(0), fail(0)
LDAP max group query period(seconds): 0
LDAP status: connected
```

```
Group Filter: CN=group2,OU=Testing,DC=Fortinet-
FSSO,DC=com+CN=group21,OU=Testing,DC=Fortinet-FSSO,DC=COM
```

If the polling frequency shows successes and failures, that indicates sporadic network problems or a very busy DC. If it indicates no successes or failures, then incorrect credentials could be the issue.

If the LDAP status is connected, then the FortiGate can access the configured LDAP server. This is required for AD group membership lookup of authenticated users because the Windows Security Event log does not include group membership information. The FortiGate sends an LDAP search for group membership of authenticated users to the configured LDAP server.

FortiGate adds authenticated users to the local FSSO user list only if the group membership is one of the groups in Group Filter.

4. If necessary, capture the output of the local FortiGate daemon that polls Windows Security Event logs:

```
diagnose debug application fssod -1
```

This output contains a lot of detailed information which can be captured to a text file.

## Limitations

- NTLM based authentication is not supported.
- If there are a large number of user log ins at the same time, the FSSO daemon may miss some. Consider using FSSO agent mode if this will be an issue. See [Fabric connectors on page 139](#) for information.
- The FSSO daemon does not support all of the security log events that are supported by other FSSO scenarios. For example, only Kerberos log in events 4768 and 4769 are supported.

## Enabling Active Directory recursive search

By default, nested groups (groups that are members of other groups) are not searched in Windows Active Directory (AD) LDAP servers because this can slow down the group membership search. There is an option in FortiOS to enable the searching of nested groups for user group memberships on AD LDAP servers.



This option is not available for other LDAP servers, such as OpenLDAP-based servers.

The default behavior does not include nested groups:

```
config user ldap
 edit "ldap-ad"
 set server "10.1.100.131"
 set cnid "cn"
 set dn "dc=fortinet-fsso,dc=com"
 set type regular
 set username "cn=Administrator,cn=users,dc=fortinet-fsso,dc=com"
 set password XXXXXXXXXXXXXXXXXXXXXXXX
 next
end
```

The default search results only show groups that have the user as member, and no groups that have groups as members:

```
diagnose test authserver ldap ldap-ad nuser nuser
 authenticate 'nuser' against 'ldap-ad' succeeded!
 Group membership(s) - CN=nested3,OU=Testing,DC=Fortinet-FSSO,DC=COM
 CN=Domain Users,CN=Users,DC=Fortinet-FSSO,DC=COM
```

**To enable recursive search to include nested groups in the results:**

```
config user ldap
 edit "ldap-ad"
 set server "10.1.100.131"
 set cnid "cn"
 set dn "dc=fortinet-fsso,dc=com"
 set type regular
 set username "cn=Administrator,cn=users,dc=fortinet-fsso,dc=com"
 set password XXXXXXXXXXXXXXXXXXXXXXXX
 set search-type recursive
```

```
 next
end
```

The search results now include groups that have other groups as members:

```
diagnose test authserver ldap ldap-ad nuser nuser
 authenticate 'nuser' against 'ldap-ad' succeeded!
 Group membership(s) - CN=nested3,OU=Testing,DC=Fortinet-FSSO,DC=COM
 CN=Domain Users,CN=Users,DC=Fortinet-FSSO,DC=COM
 CN=nested2,OU=Testing,DC=Fortinet-FSSO,DC=COM
 CN=nested1,OU=Testing,DC=Fortinet-FSSO,DC=COM
```

The group nested3 is a member of the group nested2, which is a member of the group nested1.

## Configuring LDAP dial-in using a member attribute

In this configuration, users defined in Microsoft AD can set up a VPN connection based on an attribute that is set to `TRUE`, instead of their user group. You can activate the *Allow Dialin* property in AD user properties, which sets the `msNPAllowDialin` attribute to `TRUE`. You can use this procedure for other member attributes as your system requires.

This configuration consists of the following steps:

1. Ensure that the AD server has the `msNPAllowDialin` attribute set to `TRUE` for the desired users.
2. [Configure user LDAP member attribute settings.](#)
3. [Configure LDAP group settings.](#)
4. [Ensure that you configured the settings correctly.](#)

**To configure user LDAP member attribute settings:**

```
config user ldap
 edit "ldap_server"
 set server "192.168.201.3"
 set cnid "sAMAccountName"
 set dn "DC=fortilabanz,DC=com,DC=au"
 set type regular
 set username "fortigate@sample.com"
 set password *****
 set member-attr "msNPAllowDialin"
 next
end
```

**To configure LDAP group settings:**

```
config user group
 edit "ldap_grp"
 set member "ldap_server"
 config match
 edit 1
 set server-name "ldap_server"
 set group-name "TRUE"
 next
 end
 next
end
```

**To ensure that you configured the settings correctly:**

Users that are members of the `ldap_grp` user group should be able to authenticate. The following shows sample diagnose debug output when the `Allow Dial-in` attribute is set to `TRUE`:

```
get_member_of_groups-Get the memberOf groups.
get_member_of_groups- attr='msNPAllowDialin', found 1 values
get_member_of_groups-val[0]='TRUE'
fnbamd_ldap_get_result-Auth accepted
fnbamd_ldap_get_result-Going to DONE state res=0
fnbamd_auth_poll_ldap-Result for ldap svr 192.168.201.3 is SUCCESS
fnbamd_auth_poll_ldap-Passed group matching
```

If the attribute is not set to `TRUE` but is expected, you may see the following output:

```
get_member_of_groups-Get the memberOf groups.
get_member_of_groups- attr='msNPAllowDialin', found 1 values
get_member_of_groups-val[0]='FALSE'
fnbamd_ldap_get_result-Auth accepted
fnbamd_ldap_get_result-Going to DONE state res=0
fnbamd_auth_poll_ldap-Result for ldap svr 192.168.201.3 is SUCCESS
fnbamd_auth_poll_ldap-Failed group matching
```

The difference between the two outputs is the last line, which shows passed or failed depending on whether the member attribute is set to the expected value.

## Configuring wildcard admin accounts

To avoid setting up individual admin accounts in FortiOS, you can configure an admin account with the wildcard option enabled, allowing multiple remote admin accounts to match one local admin account. This way, multiple LDAP admin accounts can use one FortiOS admin account.

Benefits include:

- Fast configuration of the FortiOS admin account to work with your LDAP network, saving effort and avoiding potential errors incurred when setting up multiple admin accounts
- Reduced ongoing maintenance. As long as LDAP users belong to the same group and you do not modify the wildcard admin account in FortiOS, you do not need to configure changes on the LDAP accounts. If you add or remove a user from the LDAP group, you do not need to perform changes in FortiOS.

Potential issues include:

- Multiple users may be logged in to the same account simultaneously. This may cause issues if both users make changes simultaneously.
- Security is reduced since multiple users have login access to the same account, as opposed to an account for each user.

Wildcard admin configuration also applies to RADIUS. If configuring for RADIUS, configure the RADIUS server and RADIUS user group instead of LDAP. When using the GUI, wildcard admin is the only remote admin account that does not require you to enter a password on account creation. That password is normally used when the remote authentication server is unavailable during authentication.

This example uses default values where possible. If a specific value is not mentioned, the example sets it to its default value.



You can configure an admin account in Active Directory for LDAP authentication to allow an admin to perform lookups and reset passwords without being a member of the Account Operators or Domain Administrators built-in groups. See [Configuring least privileges for LDAP admin account authentication in Active Directory on page 1520](#).

### To configure the LDAP server:

The important parts of this configuration are the username and group lines. The username is the domain administrator account. The group binding allows only the GRP group access.

This example uses an example domain name. Configure as appropriate for your own network.

```
config user ldap
 edit "ldap_server"
 set server "192.168.201.3"
 set cnid "sAMAccountName"
 set dn "DC=example,DC=com,DC=au"
 set type regular
 set username "CN=Administrator,CN=Users,DC=example,DC=COM"
 set password *
 set group-member-check group-object
 set group-object-filter (&
 (objectcategory=group)member="CN=GRP,OU=training,DC=example,DC=COM")
 next
end
```

### To configure the user group and add the LDAP server:

```
config user group
 edit "ldap_grp"
 set member "ldap_server"
 config match
 edit 1
 set server-name "ldap_server"
 set group-name "CN=GRP,OU=training,DC=example,DC=COM"
 next
 end
 next
end
end
end
end
```

### To configure the wildcard admin account:

```
config system admin
 edit "test"
 set remote-auth enable
 set accprofile "super_admin"
 set wildcard enable
 set remote-group "ldap_grp"
 next
end
```

## Configuring least privileges for LDAP admin account authentication in Active Directory

An administrator should only have sufficient privileges for their role. In the case of LDAP admin bind, you can configure an admin account in Active Directory for LDAP authentication to allow an admin to perform lookups and reset passwords without being a member of the Account Operators or Domain Administrators built-in groups.

For information about Active Directory, see the [product documentation](#).

### To configure account privileges for LDAP authentication in Active Directory:

1. In the *Active Directory Users and Computers* administrative console, right-click the Organizational Unit (OU) or the top-level domain you want to configure and select *Delegate Control*.
2. In the *Delegation of Control Wizard* dialog, click *Next*.
3. In the *Users or Groups* dialog, click *Add...* and search Active Directory for the users or groups.
4. Click *OK* and then click *Next*.
5. In the *Tasks to Delegate* dialog, select *Create a custom task to delegate* and click *Next*.
6. Select *Only the following objects in the folder* and scroll to the bottom of the list. Select *User objects* and click *Next*.
7. In the *Permissions* dialog, select *General*.
8. From the *Permissions* list, select the following:
  - *Change password*
  - *Reset password*
9. Clear the *General* checkbox and select *Property-specific*.
10. From the *Permissions* list, select the following:
  - *Write lockoutTime*
  - *Read lockoutTime*
  - *Write pwdLastSet*
  - *Read pwdLastSet*
  - *Write UserAccountControl*
  - *Read UserAccountControl*
11. Click *Next* and click *Finish*.

## RADIUS Servers

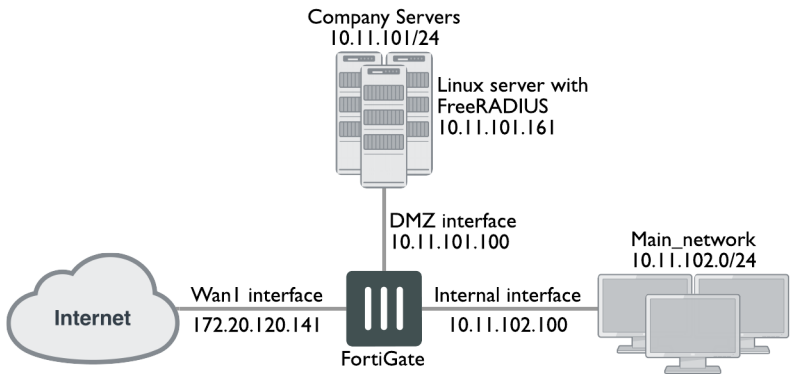
### Configuring RADIUS SSO authentication

A common RADIUS SSO (RSSO) topology involves a medium-sized company network of users connecting to the Internet through the FortiGate and authenticating with a RADIUS server. The following describes how to configure FortiOS for this scenario. The example makes the following assumptions:

- VDOMs are not enabled.
- The super\_admin account is used for all FortiGate configuration.
- A RADIUS server is installed on a server or FortiAuthenticator and uses default attributes.
- BGP is used for any dynamic routing.
- You have configured authentication event logging under *Log & Report*.

Example.com has an office with 20 users on the internal network who need access to the Internet. The office network is protected by a FortiGate-60C with access to the Internet through the wan1 interface, the user network on the internal interface, and all servers are on the DMZ interface. This includes an Ubuntu sever running FreeRADIUS. This example configures two users:

User	Account
Pat Lee	plee@example.com
Kelly Green	kgreen@example.com



Configuring this example consists of the following steps:

1. [Configure RADIUS.](#)
2. [Configure FortiGate interfaces.](#)
3. [Configure a RSSO agent.](#)
4. [Create a RSSO user group.](#)
5. [Configure security policies.](#)
6. [Test the configuration.](#)

**To configure RADIUS:**

Configuring RADIUS includes configuring a RADIUS server such as FreeRADIUS on user's computers and configuring users in the system. In this example, Pat and Kelly belong to the `exampledotcom_employees` group. After completing the configuration, you must start the RADIUS daemon. The users have a RADIUS client installed on their PCs that allow them to authenticate through the RADIUS server.

For any problems installing FreeRADIUS, see the [FreeRADIUS documentation](#).

**To configure FortiGate interfaces:**

You must define a DHCP server for the internal network, as this network type typically uses DHCP. The wan1 and dmz interfaces are assigned static IP addresses and do not need a DHCP server. The following table shows the FortiGate interfaces used in this example:

Interface	Subnet	Act as DHCP server	Devices
wan1	172.20.120.141	No	Internet service provider
dmz	10.11.101.100	No	Servers including

Interface	Subnet	Act as DHCP server	Devices
			RADIUS server
internal	10.11.102.100	Yes: x.x.x.110-250	Internal user network

1. Go to *Network > Interfaces*.
2. Edit wan1:

<b>Alias</b>	Internet
<b>Addressing Mode</b>	Manual
<b>IP/Network Mask</b>	172.20.120.141/255.255.255.0
<b>Administrative Access</b>	HTTPS, SSH
<b>Enable DHCP Server</b>	Not selected
<b>Comments</b>	Internet
<b>Administrative Status</b>	Up

3. Click *OK*.
4. Edit dmz:

<b>Alias</b>	Servers
<b>Addressing Mode</b>	Manual
<b>IP/Network Mask</b>	10.11.101.100/255.255.255.0
<b>Administrative Access</b>	HTTPS, SSH, PING, SNMP
<b>Enable DHCP Server</b>	Not selected
<b>Listen for RADIUS Accounting Messages</b>	Select
<b>Comments</b>	Servers
<b>Administrative Status</b>	Up

5. Click *OK*.
6. Edit internal:

<b>Alias</b>	Internal network
<b>Addressing Mode</b>	Manual
<b>IP/Network Mask</b>	10.11.102.100/255.255.255.0
<b>Administrative Access</b>	HTTPS, SSH, PING
<b>Enable DHCP Server</b>	Select
<b>Address Range</b>	10.11.102.110 - 10.11.102.250
<b>Netmask</b>	255.255.255.0



<b>Default Gateway</b>	Same as Interface IP
<b>Comments</b>	Internal network
<b>Administrative Status</b>	Up

#### To create a RADIUS SSO agent:

1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New*.
3. Under *SSO/Identity*, select *RADIUS Single Sign-On Agent*.
4. Enable *Use RADIUS Shared Secret*. Enter the RADIUS server's shared secret.
5. Enable *Send RADIUS Responses*. Click *OK*.

#### To create a RADIUS SSO user group:

1. Go to *User & Device > User Groups*.
2. Click *Create New*.
3. For *Type*, select *RADIUS Single Sign-On (RSSO)*.
4. In *RADIUS Attribute Value*, enter the name of the RADIUS user group that this local user group represents.
5. Click *OK*.

### Configuring security policies

The following security policies are required for RADIUS SSO:

Sequence Number	From	To	Type	Schedule	Description
1	internal	wan1	RADIUS SSO	Business hours	Authenticate outgoing user traffic
2	internal	wan1	Regular	Always	Allow essential network services and VoIP
3	dmz	wan1	Regular	Always	Allow servers to access the Internet
4	internal	dmz	Regular	Always	Allow users to access servers
5	any	any	Deny	Always	Implicit policy denying all traffic that has not been matched

You must place the RADIUS SSO policy at the top of the policy list so that it is matched first. The only exception to this is if you have a policy to deny access to a list of banned users. In this case, you must put that policy at the top so that the RADIUS SSO does not mistakenly match a banned user or IP address.

You must configure lists before creating security policies.

## Schedule

You must configure a business\_hours schedule. You can configure a standard Monday to Friday 8 AM to 5 PM schedule, or whatever days and hours covers standard work hours at the company.

## Address groups

You must configure the following address groups:

Name	Interface	Address range included
internal_network	internal	10.11.102.110 to 10.11.102.250
company_servers	dmz	10.11.101.110 to 10.11.101.250

## Service groups

You must configure the service groups. The services listed are suggestions and you may include more or less as required:

Name	Interface	Description of services to be included
essential_network_services	internal	Any network protocols required for normal network operation such as DNS, NTP, BGP
essential_server_services	dmz	All the protocols required by the company servers such as BGP, HTTP, HTTPS, FTP, IMAP, POP3, SMTP, IKE, SQL, MYSQL, NTP, TRACEROUTE, SOCKs, and SNMP
user_services	internal	Any protocols required by users such as HTTP, HTTPS, FTP

The following security policy configurations are basic and only include logging and default AV and IPS. These policies allow or deny access to non-RADIUS SSO traffic. These are essential as network services including DNS, NTP, and FortiGuard require access to the Internet.

### To configure security policies:

1. Go to *Policy & Objects > IPv4 Policy*.
2. Click *Create New*.
3. Configure the policy as follows, then click *OK*:

<b>Incoming Interface</b>	Internal
<b>Source Address</b>	internal_network
<b>Outgoing Interface</b>	wan1
<b>Destination Address</b>	all
<b>Schedule</b>	always

<b>Service</b>	essential_network_services
<b>Action</b>	ACCEPT
<b>NAT</b>	ON
<b>Security Profiles</b>	ON: AntiVirus, IPS
<b>Log Allowed Traffic</b>	ON
<b>Comments</b>	Essential network services

4. Click *Create New*, and configure the new policy as follows, then click *OK*:

<b>Incoming Interface</b>	dmz
<b>Source Address</b>	company_servers
<b>Outgoing Interface</b>	wan1
<b>Destination Address</b>	all
<b>Schedule</b>	always
<b>Service</b>	essential_server_services
<b>Action</b>	ACCEPT
<b>NAT</b>	ON
<b>Security Profiles</b>	ON: AntiVirus, IPS
<b>Log Allowed Traffic</b>	enable
<b>Comments</b>	Company servers accessing the Internet

5. Click *Create New*, and configure the new policy as follows, then click *OK*:

<b>Incoming Interface</b>	Internal
<b>Source Address</b>	internal_network
<b>Outgoing Interface</b>	dmz
<b>Destination Address</b>	company_servers
<b>Schedule</b>	always
<b>Service</b>	all
<b>Action</b>	ACCEPT
<b>NAT</b>	ON
<b>Security Profiles</b>	ON: AntiVirus, IPS
<b>Log Allowed Traffic</b>	enable
<b>Comments</b>	Access company servers

6. Click *Create New*, and configure the RADIUS SSO policy as follows, then click *OK*. This policy allows access for members of specific RADIUS groups.

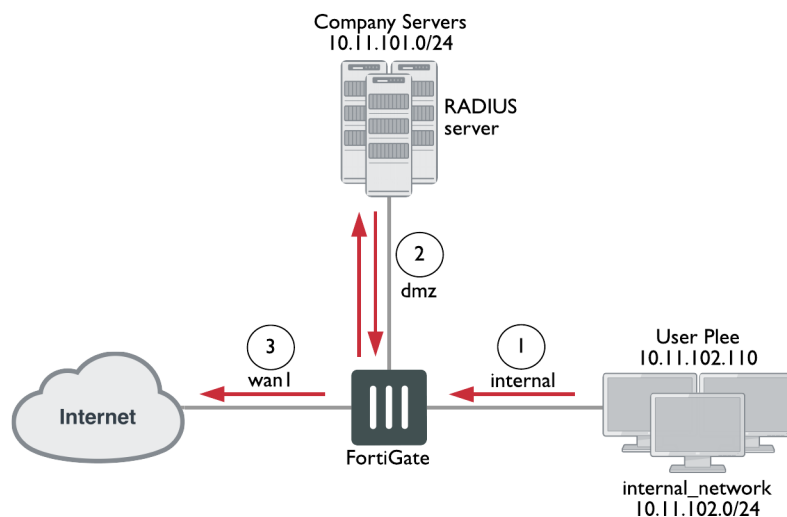
<b>Incoming Interface</b>	Internal
<b>Source Address</b>	internal_network
<b>Source User(s)</b>	Select the user groups that you created for RSSO.
<b>Outgoing Interface</b>	wan1
<b>Destination Address</b>	all
<b>Schedule</b>	business_hours
<b>Service</b>	ALL
<b>Action</b>	ACCEPT
<b>NAT</b>	ON
<b>Security Profiles</b>	ON: AntiVirus, Web Filter, IPS, and Email Filter. In each case, select the default profile.

7. Place the RSSO policy higher in the security policy list than more general policies for the same interfaces. Click **OK**.

### To test the configuration:

Once configured, a user only needs to log in to their PC using their RADIUS account. After that, when they attempt to access the Internet, the FortiGate uses their session information to get their RADIUS information. Once the user is verified, they can access the website.

1. The user logs on to their PC and tries to access the Internet.
2. The FortiGate contacts the RADIUS server for the user's information. Once confirmed, the user can access the Internet. Each step generates logs that enable you to verify that each step succeeded.
3. If a step does not succeed, confirm that your configuration is correct.



## RSA ACE (SecurID) servers

SecurID is a two-factor system produced by the company RSA that uses one-time password (OTP) authentication. This system consists of the following:

- Portable tokens that users carry
- RSA ACE/Server
- Agent host (the FortiGate)

When using SecurID, users carry a small device or "token" that generates and displays a pseudo-random password. According to RSA, each SecurID authenticator token has a unique 64-bit symmetric key that is combined with a powerful algorithm to generate a new code every 60 seconds. The token is time-synchronized with the SecurID RSA ACE/Server.

The RSA ACE/Server is the SecurID system's management component. It stores and validates the information about the SecurID tokens allowed on your network. Alternately, the server can be an RSA SecurID 130 appliance.

The agent host is the server on your network. In this case, this is the FortiGate, which intercepts user logon attempts. The agent host gathers the user ID and password entered from the SecurID token and sends the information to the RSA ACE/Server for validation. If valid, the RSA ACE/Server returns a reply indicating that it is a valid logon and FortiOS allows the user access to the network resources specified in the associated security policy.

Configuring SecurID with FortiOS consists of the following:

1. Configure the RSA and RADIUS servers to work with each other. See RSA server documentation.
2. Do one of the following:
  - a. [Configure the RSA SecurID 130 appliance.](#)
  - b. [Configure the FortiGate as an agent host on the RSA ACE/Server.](#)
3. [Configure the RADIUS server in FortiOS.](#)
4. [Create a SecurID user group.](#)
5. [Create a SecurID user.](#)
6. [Configure authentication with SecurID.](#)

The following instructions are based on RSA ACE/Server 5.1 and RSA SecurID 130 appliance. They assume that you have successfully completed all external RSA and RADIUS server configuration.

In this example, the RSA server is on the internal network and has an IP address of 192.128.100.000. The FortiOS internal interface address is 192.168.100.3. The RADIUS shared secret is fortinet123, and the RADIUS server is at IP address 192.168.100.202.

#### To configure the RSA SecurID 130 appliance:

1. Log on to the SecurID IMS console.
2. Go to *RADIUS > RADIUS clients*, then select *Add New*.

Setting	Description
<b>RADIUS Client Basics</b>	
Client Name	FortiGate
Associated RSA Agent	FortiGate
<b>RADIUS Client Settings</b>	
IP Address	Enter the FortiOS internal interface. In this example, it is 192.168.100.3.
Make / Model	Select <i>Standard Radius</i> .
Shared Secret	Enter the RADIUS shared secret. In this example, it is fortinet123.

Setting	Description
Accounting	Leave unselected.
Client Status	Leave unselected.

3. Configure your FortiGate as a SecurID client:
4. Click **Save**.

#### To configure the FortiGate as an agent host on the RSA ACE/Server:

1. On the RSA ACE/Server, go to *Start > Programs > RSA ACE/Server*, then *Database Administration - Host Mode*.
2. From the *Agent Host* menu, select *Add Agent Host*.
3. Configure the following:

Setting	Description
Name	FortiGate
Network Address	Enter the FortiOS internal interface. In this example, it is 192.168.100.3.
Secondary Nodes	You can optionally enter other IP addresses that resolve to the FortiGate.

For more information, see the RSA ACE/Server documentation.

#### To configure the RADIUS server in FortiOS:

1. Go to *User & Device > RADIUS Servers*, then click *Create New*.
2. Configure the following:

Setting	Description
Name	RSA
Authentication method	Select <i>Default</i> .
<b>Primary Server</b>	
IP/Name	192.168.100.102. You can click <i>Test</i> to ensure the IP address is correct and that FortiOS can contact the RADIUS server.
Secret	fortinet123

3. Click **OK**.

#### To create a SecurID user group:

1. Go to *User & Device > User Groups*. Click *Create New*.
2. Configure the following:

Setting	Description
Name	RSA_group
Type	Firewall

3. In *Remote Groups*, click *Add*, then select the RSA server.
4. Click *OK*.

**To create a SecurID user:**

1. Go to *User & Device > User Definition*. Click *Create New*.
2. Configure the following:

Setting	Description
User Type	Remote RADIUS User
Type	wloman
RADIUS Server	RSA
Contact Info	(Optional) Enter email or SMS information.
User Group	RSA_group

3. Click *Create*.

You can test the configuration by entering the `diagnose test authserver radius RSA auto wloman 1111111111` command. The series of 1s is the OTP that your RSA SecurID token generates that you enter for access.

## Configuring authentication with SecurID

You can use the SecurID user group in several FortiOS features that authenticate by user group:

- [Security policy on page 1529](#)
- [IPsec VPN XAuth on page 1530](#)
- [PPTP VPN on page 1530](#)
- SSL VPN

Unless stated otherwise, the following examples use default values.

### Security policy

The example creates a security policy that allows HTTP, FTP, and POP3 traffic from the internal interface to WAN1. If these interfaces are not available in FortiOS, substitute other similar interfaces.

**To configure a security policy with SecurID authentication:**

1. Go to *Policy & Objects > IPv4 Policy*.
2. Click *Create New*.

**3. Configure the following:**

Setting	Description
Incoming Interface	internal
Source Address	all
Source User(s)	RSA_group
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	HTTP, FTP, POP3
Action	ACCEPT
NAT	On
Shared Shaper	If you want to limit traffic or guarantee minimum bandwidth for traffic that uses the SecurID security policy, enable and use the default shaper, guarantee-100kbps.
Log Allowed Traffic	Enable if you want to generate usage reports on traffic that this policy has authenticated.

**4. Click OK.****IPsec VPN XAuth**

In *VPN > IPsec Wizard*, select the SecurID user group on the *Authentication* page. The SecurID user group members must enter their SecurID code to authenticate.

**PPTP VPN**

When configuring PPTP in the CLI, set `usrgrp` to the SecurID user group.

**SSL VPN**

You must map the SecurID user group to the portal that will serve SecurID users and include the SecurID user group in the security policy's *Source User(s)* field.

**To map the SecurID group to an SSL VPN portal:**

1. Go to *VPN > SSL-VPN Settings*.
2. Under *Authentication/Portal Mapping*, click *Create New*.



3. Configure the following:

Setting	Description
Users/Groups	RSA_group
Portal	Select the desired portal.

4. Click OK.

## TACACS+ Servers

TACACS+ is a remote authentication protocol that provides access control for routers, network access servers, and other network devices through one or more centralized servers.

FortiOS sends the following proprietary TACACS+ attributes to the TACACS+ server during authorization requests:

Attribute	Description
service=<name>	User must be authorized to access the specified service.
memberof	Group that the user belongs to.
admin_prof	Administrator profile (admin access only).



Only `memberof` and `admin_prof` attributes are parsed in authentication replies.

You can configure up to ten remote TACACS+ servers in FortiOS. You must configure at least one server before you can configure remote users.



A TACACS+ server must first be added in the CLI to make the option visible in the GUI.

### To configure TACACS+ authentication in the CLI:

1. Configure the TACACS+ server entry:

```
config user tacacs+
 edit "TACACS-SERVER"
 set server <IP address>
 set key <string>
 set authen-type ascii
 set source-ip <IP address>
 next
end
```

**2. Configure the remote user group:**

```
config user group
 edit "TACACS-GROUP"
 set group-type firewall
 set member "TACACS-SERVER"
 next
end
```

**3. Configure the remote user:**

```
config system admin
 edit TACACS-USER
 set remote-auth enable
 set accprofile "super_admin"
 set vdom "root"
 set wildcard enable
 set remote-group "TACACS-GROUP"
 next
end
```

**To configure a TACACS+ server in the GUI:**

1. Go to *User & Device > TACACS+ Servers*.
2. Click *Create New*.
3. Configure the following settings:

<b>Name</b>	Enter the TACACS+ server name.
<b>Authentication Type</b>	Select the authentication type used for the TACACS+ server. Selecting <i>Auto</i> tries PAP, MSCHAP, and CHAP, in that order.
<b>Server IP/Name</b>	Enter the domain name or IP address for the primary server.
<b>Server Secret</b>	Enter the key to access the primary server.

4. Click *OK*.

## Authentication Settings

You can configure general authentication settings, including timeout, protocol support, and certificates.

---



You cannot customize FTP and Telnet authentication replacement messages.

---

**To configure authentication settings using the GUI:**

1. Go to *User & Device > Authentication Settings*.
2. Configure the following settings:

Setting	Description
Authentication Timeout	Enter the desired timeout in minutes. You can enter a number between 1 and 1440 (24 hours). The authentication timeout controls how long an authenticated connection can be idle before the user must reauthenticate. The default value is 5.
Protocol Support	<p>Select the protocols to challenge during firewall user authentication. When you enable user authentication within a security policy, the authentication challenge is normally issued for any of four protocols, depending on the connection protocol:</p> <ul style="list-style-type: none"> <li>• HTTP (you can set this to redirect to HTTPS)</li> <li>• HTTPS</li> <li>• FTP</li> <li>• Telnet</li> </ul> <p>The protocols selected here control which protocols support the authentication challenge. Users must connect with a supported protocol first so they can subsequently connect with other protocols. If HTTPS is selected as a protocol support method, it allows the user to authenticate with a customized local certificate.</p> <p>When you enable user authentication within a security policy, FortiOS challenges the security policy user to authenticate. For user ID and password authentication, the user must provide their username and password. For certificate authentication (HTTPS or HTTP redirected to HTTPS only), you can install customized certificates on the unit and the user can also install customized certificates on their browser. Otherwise, users see a warning message and must accept a default Fortinet certificate. The network user's web browser may deem the default certificate invalid.</p>
Certificate	If using HTTPS protocol support, select the local certificate to use for authentication. This is available only if <i>HTTPS</i> and/or <i>Redirect HTTP Challenge to a Secure Channel (HTTPS)</i> are selected.

**To configure authentication settings using the CLI:**

```
config user setting
 set auth-timeout 5
 set auth-type ftp http https telnet
 set auth-cert Fortinet_Factory
end
```

## FortiTokens

FortiTokens are security tokens used as part of a multi-factor authentication (MFA) system on FortiGate and FortiAuthenticator. A security token is a 6-digit or 8-digit (configurable) one-time password (OTP) that is used to authenticate one's identity electronically as a prerequisite for accessing network resources. FortiToken is available as either a mobile or a physical (hard) token. Mobile tokens can be purchased as a license, or consumed with points as part of the FortiToken Cloud service.

FortiToken Mobile and physical FortiTokens store their encryption seeds on the cloud. FortiToken Mobile seeds are generated dynamically when the token is provisioned. They are always encrypted whether in motion or at rest.

You can only register FortiTokens to a single FortiGate or FortiAuthenticator for security purposes. This prevents malicious third parties from making fraudulent requests to hijack your FortiTokens by registering them on another FortiGate or FortiAuthenticator. If re-registering a FortiToken Mobile or Hard Token on another FortiGate is required, you must contact [Fortinet Customer Support](#).

Common usage for FortiTokens includes:

- Applying MFA to a VPN dialup user connecting to the corporate network
- Applying MFA to FortiGate administrators
- Applying MFA to firewall authentication and captive portal authentication



The MFA process commonly involves:

- **Something you know:** User password
- **Something you have:** The FortiToken OTP

A third factor of authentication is added to the authentication process:

- **Something you are:** Your fingerprint or face

To enable the third factor, refer to the [Activating FortiToken Mobile on a Mobile Phone on page 1539](#) section.

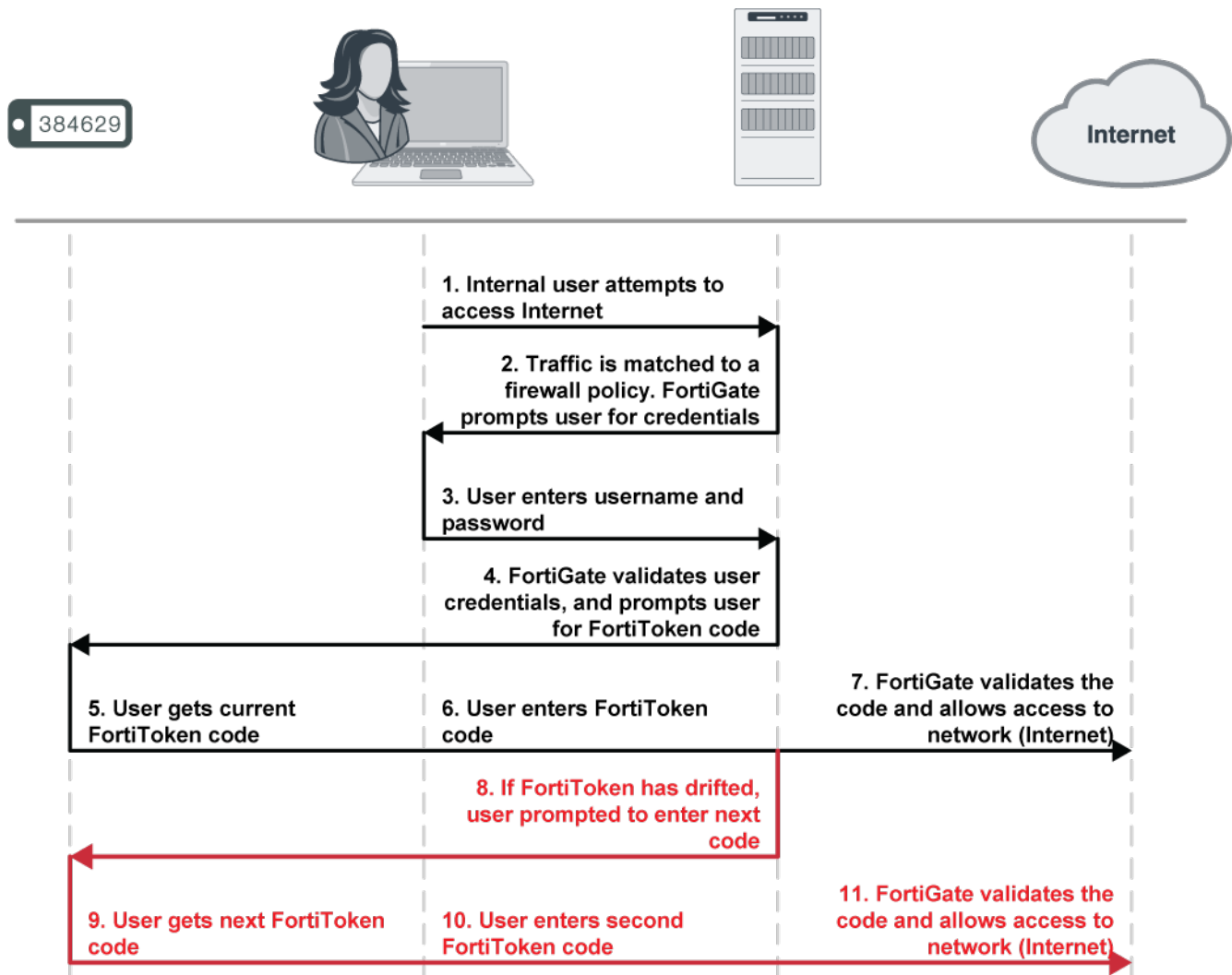
---

### The following illustrates the FortiToken MFA process:

1. The user attempts to access a network resource.
2. FortiOS matches the traffic to an authentication security policy and prompts the user for their username and password.
3. The user enters their username and password.
4. FortiOS verifies their credentials. If valid, it prompts the user for the FortiToken code.
5. The user views the current code on their FortiToken. They enter the code at the prompt.
6. FortiOS verifies the FortiToken code. If valid, it allows the user access to network resources.

### If the FortiToken has drifted, the following must take place for the FortiToken to resynchronize with FortiOS:

1. FortiOS prompts the user to enter a second code to confirm.
2. The user gets the next code from the FortiToken. They enter the code at the prompt.
3. FortiOS uses both codes to update its clock to match the FortiToken.



This section includes the following topics to quickly get started with FortiTokens:

- [FortiToken Mobile Quick Start Guide on page 1535](#)
- [FortiToken Cloud on page 1546](#)
- [Registering hard tokens on page 1547](#)
- [Managing FortiTokens on page 1549](#)
- [FortiToken Mobile Push on page 1551](#)
- [Troubleshooting and diagnosis on page 1553](#)

## FortiToken Mobile Quick Start Guide

FortiToken Mobile is an OATH compliant, event- and time-based one-time password (OTP) generator for mobile devices. It provides an easy and flexible way to deploy and provision FortiTokens to your end users through mobile devices. FortiToken Mobile produces its OTP codes in an application that you can download onto your Android or iOS mobile device without the need for a physical token.

You can download the free FortiToken Mobile application for Android from the [Google Play Store](#), and for iOS from the [Apple App Store](#).

This section focuses on quickly getting started and setting up FortiToken Mobile for use on a FortiGate:

- [Registering FortiToken Mobile on page 1536](#)
- [Provisioning FortiToken Mobile on page 1537](#)
- [Activating FortiToken Mobile on a Mobile Phone on page 1539](#)
- [Applying Multi-Factor Authentication on page 1546](#)

## Registering FortiToken Mobile

To deploy FortiToken Mobile for your end users, you must first register the tokens on your FortiGate. After registering the tokens, you can assign them to your end users.

Each FortiGate comes with two free FortiToken Mobile tokens. These tokens should appear under *User & Device > FortiTokens*. If no tokens appear, you may import them. Ensure that your FortiGate is registered and has internet access to connect to the FortiToken servers to import the tokens.

### To import FortiTokens from the FortiGate GUI:

1. Go to *User & Device > FortiTokens*.
2. Click the *Import Free Trial Tokens* icon at the top. The two free tokens are imported.

### To import FortiTokens from the FortiGate CLI:

```
exec fortitoken-mobile import 0000-0000-0000-0000-0000
show user fortitoken
```



If only one free token appears, you can first delete that token and then follow the procedure to import the two free tokens from either the GUI or the CLI.

---

If you have the FortiToken Mobile redemption certificate, you can register FortiToken Mobile on a FortiGate.

### To register FortiToken Mobile from the FortiGate GUI:

1. Go to *User & Device > FortiTokens* and click *Create New*. The *New FortiToken* dialog appears.
2. For the *Type* field, select *Mobile Token*.
3. Locate the 20-digit code on the redemption certificate and type it in the *Activation Code* field.
4. Click *OK*. The token is successfully registered.



If you attempt to add invalid FortiToken serial numbers, there is no error message. FortiOS does not add invalid serial numbers to the list.

---

### To register FortiToken Mobile from the FortiGate CLI:

```
exec fortitoken-mobile import <20-digit activation code>
show user fortitoken
```



FortiToken Mobile stores its encryption seeds on the cloud. You can only register it to a single FortiGate or FortiAuthenticator.

## Provisioning FortiToken Mobile

Once registered, FortiTokens need to be provisioned for users before they can be activated. In this example, you will provision a Mobile token for a local user. Similar steps can be taken to assign FortiTokens to other types of users.

### To create a local user and assign a FortiToken in the FortiGate GUI:

1. Go to *User & Device > User Definition*, and click *Create New*. The *Users/Groups Creation Wizard* appears.
2. In the *User Type* tab, select *Local User*, and click *Next*.

#### Users/Groups Creation Wizard

1 User Type > 2 Login Credentials > 3 Contact Info > 4 Extra Info

Local User

Remote RADIUS User

Remote TACACS+ User

Remote LDAP User

FSSO

FortiClient EMS User

FortiNAC User

< Back

Next

Cancel

3. In the *Login Credentials* tab, enter a *Username* and *Password* for the user, and click *Next*.

#### Users/Groups Creation Wizard

✓ User Type > 2 Login Credentials > 3 Contact Info > 4 Extra Info

Username

Password

< Back

Next

Cancel

4. In the *Contact Info* tab:
  - a. Enter the user's email address in the *Email Address* field. This is the email where the user will receive the QR code for activation of the FortiToken.
  - b. Enable the *Two-factor Authentication* toggle.
  - c. Select *FortiToken* for *Authentication Type*.
  - d. Select a *Token* to assign to the user from the drop-down list.
  - e. Click *Next*.

Users/Groups Creation Wizard

☒ User Type > 
 ☒ Login Credentials > 
 **3 Contact Info** > 
 4 Extra Info

Email Address

☐ SMS

☒ Two-factor Authentication

Authentication Type FortiToken

Token FTKMOB

5. In the *Extra Info* tab, make sure the *User Account Status* field is set to Enabled. You can also optionally assign the user to a user group by enabling the *User Group* toggle.

Users/Groups Creation Wizard

☒ User Type > 
 ☒ Login Credentials > 
 ☒ Contact Info > 
 **4 Extra Info**

User Account Status Enabled Disabled

User Group ☐

6. Click *Submit*. An activation code should be sent to the created user by email or SMS, depending upon the delivery method configured above.



FortiGate has the *Email Service* setting configured using the server *notifications.fortinet.net* by default. To see configuration, go to *System > Settings > Email Service*.



The activation code expires if not activated within the 3-day time period by default. However, the expiry time period is configurable.

### To configure the time period (in hours) for FortiToken Mobile, using the CLI:

```
config system global
 set two-factor-ftm-expiry <1-168>
end
```




To resend the email or SMS with the activation code, refer to the [Managing FortiTokens on page 1549](#) section.

## Activating FortiToken Mobile on a Mobile Phone

After your system administrator provisions your token, you receive a notification with an activation code and expiry date via SMS or email. If you do not activate your token by the expiry date, you must contact your system administrator so that they can reassign your token for activation.

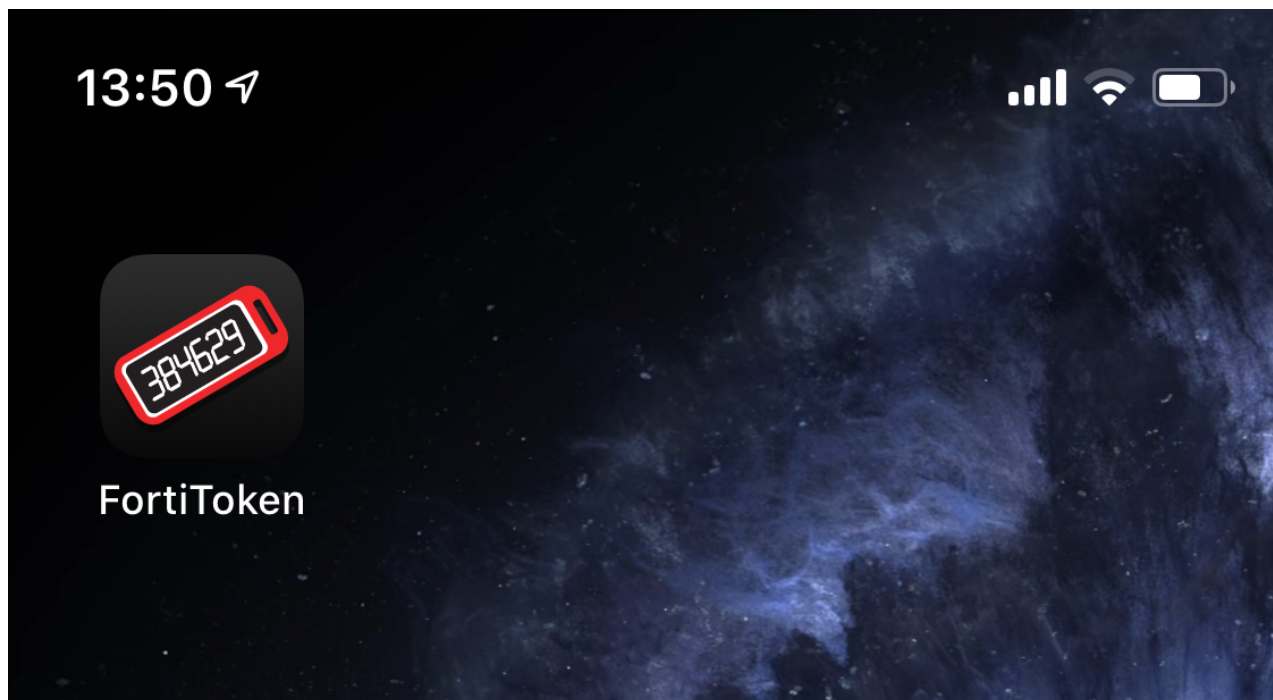
Platforms that support FortiToken Mobile:

Platform	Device and firmware support
iOS	iPhone, iPad, and iPod Touch with iOS 6.0 and later.
Android	Phones and tablets with Android Jellybean 4.1 and later.
Windows	Windows 10 (desktop and mobile), Windows Phone 8.1, and Windows Phone 8.
	 <p>FortiToken is a Windows Universal Platform (UWP) application. To download FortiToken for Windows 10 desktop and mobile platforms, see <a href="#">FortiToken for Windows on the Microsoft Store</a>.</p>

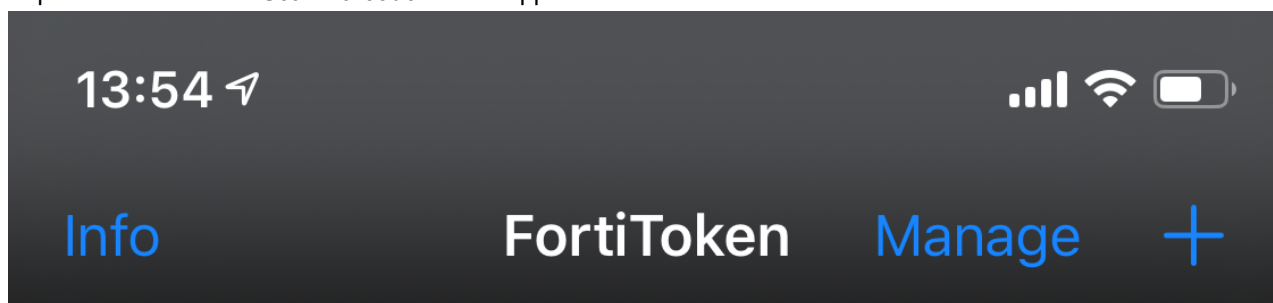
The following instructions describe procedures when using FortiToken Mobile for iOS on an iPhone. Procedures may vary depending on your device and firmware.

### To activate FortiToken Mobile on iOS:

1. On your iOS device, tap on the FortiToken application icon to open the application. If this is your first time opening the application, it may prompt you to create a PIN for secure access to the application and tokens.



2. Tap on the + icon. The *Scan Barcode* screen appears.



3. If you received the QR code via email, locate and scan the QR code in your email.  
**OR**  
If you received the activation key via SMS, tap on *Enter Manually* at the bottom of the screen, and tap on *Fortinet*.

13:55

Back Enter Manually

FORTINET ACCT

Fortinet >

Enter your email address in the *Name* field, the activation key in the *Key* field, and tap *Done*.

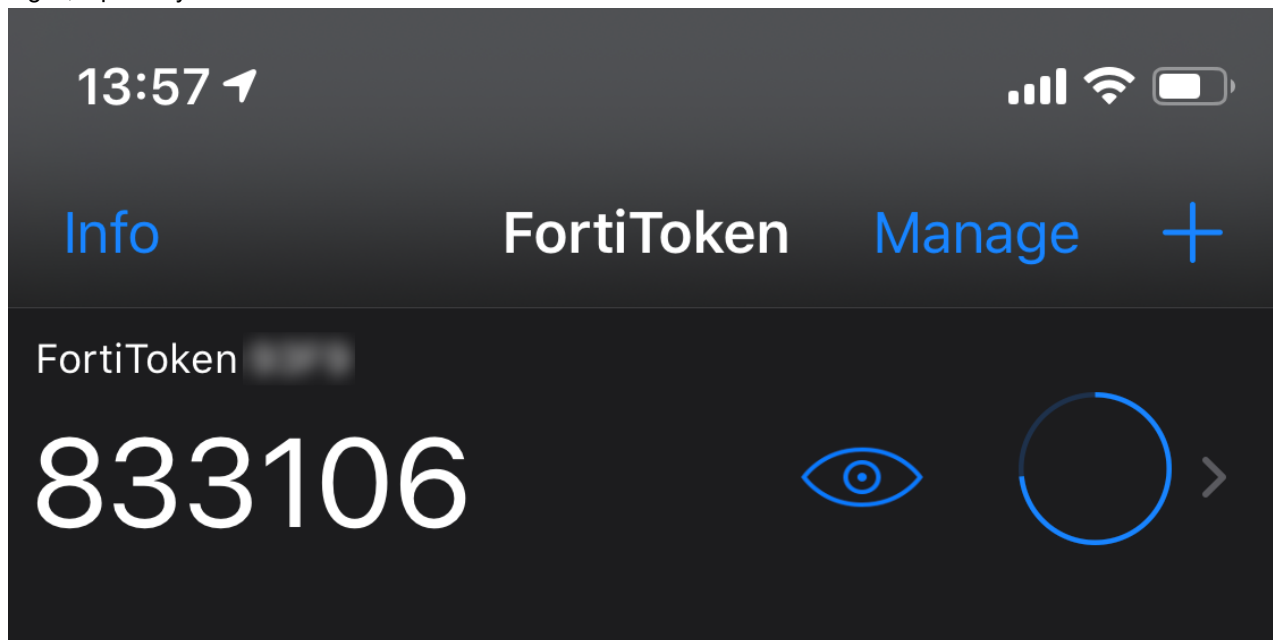
13:56

Back Fortinet Done

**Name** user@example.com

**Key** ABCD EFGH IJKL MNOP

4. FortiToken Mobile activates your token, and starts generating OTP digits immediately. To view or hide the OTP digits, tap the eye icon.

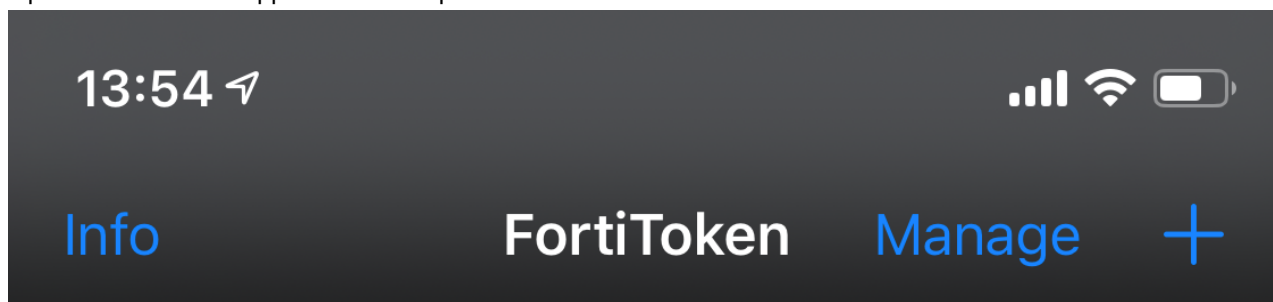


After you open the application, FortiToken Mobile generates a new 6-digit OTP every 30 seconds. All configured tokens display on the application homescreen.

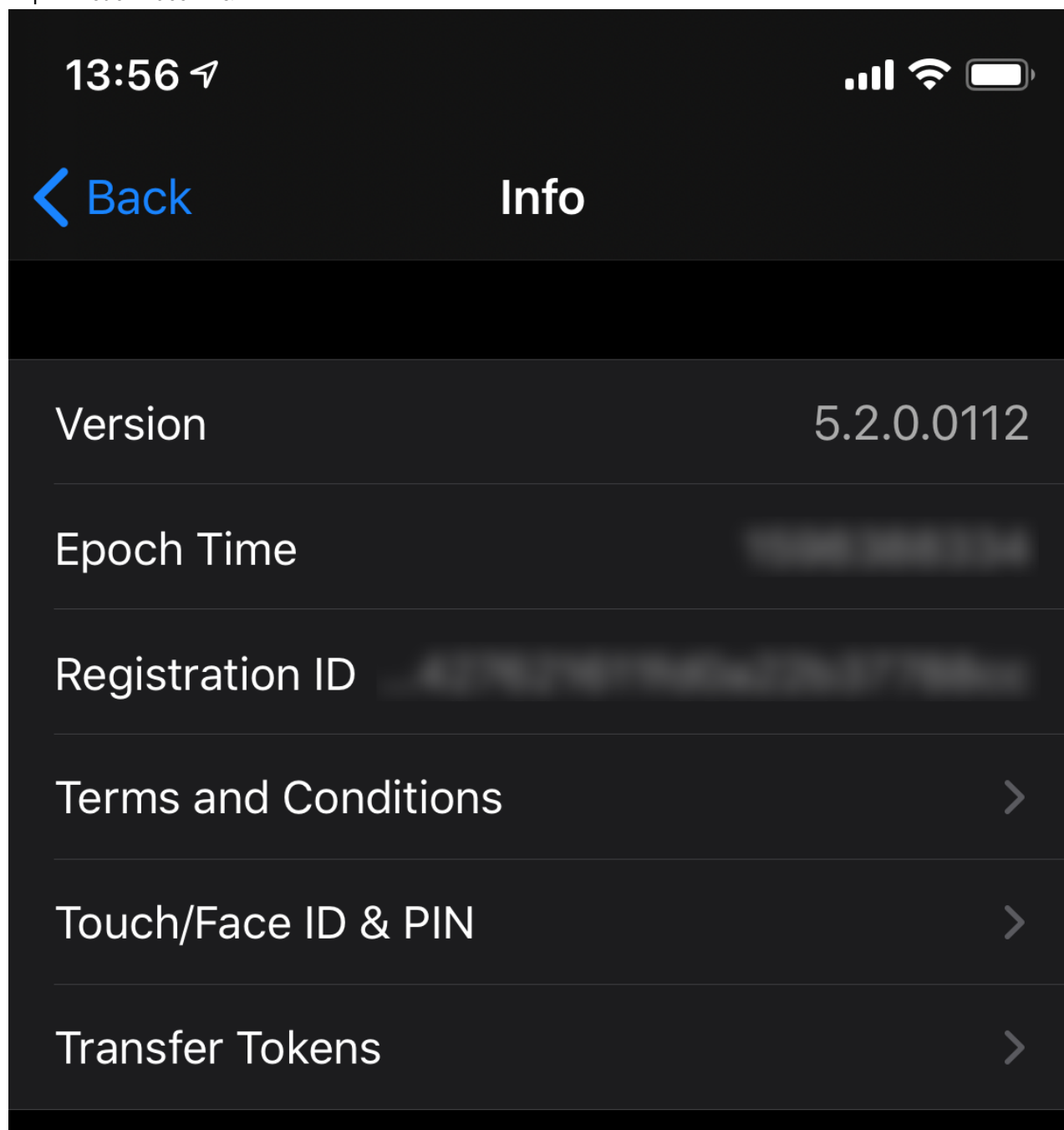
The FortiToken Mobile activation process described above caters to the MFA process that involves two factors (password and OTP) of the authentication process. A third factor (fingerprint or face) can be enabled as well.

**To enable *Touch/Face ID* on iOS for FortiToken Mobile:**

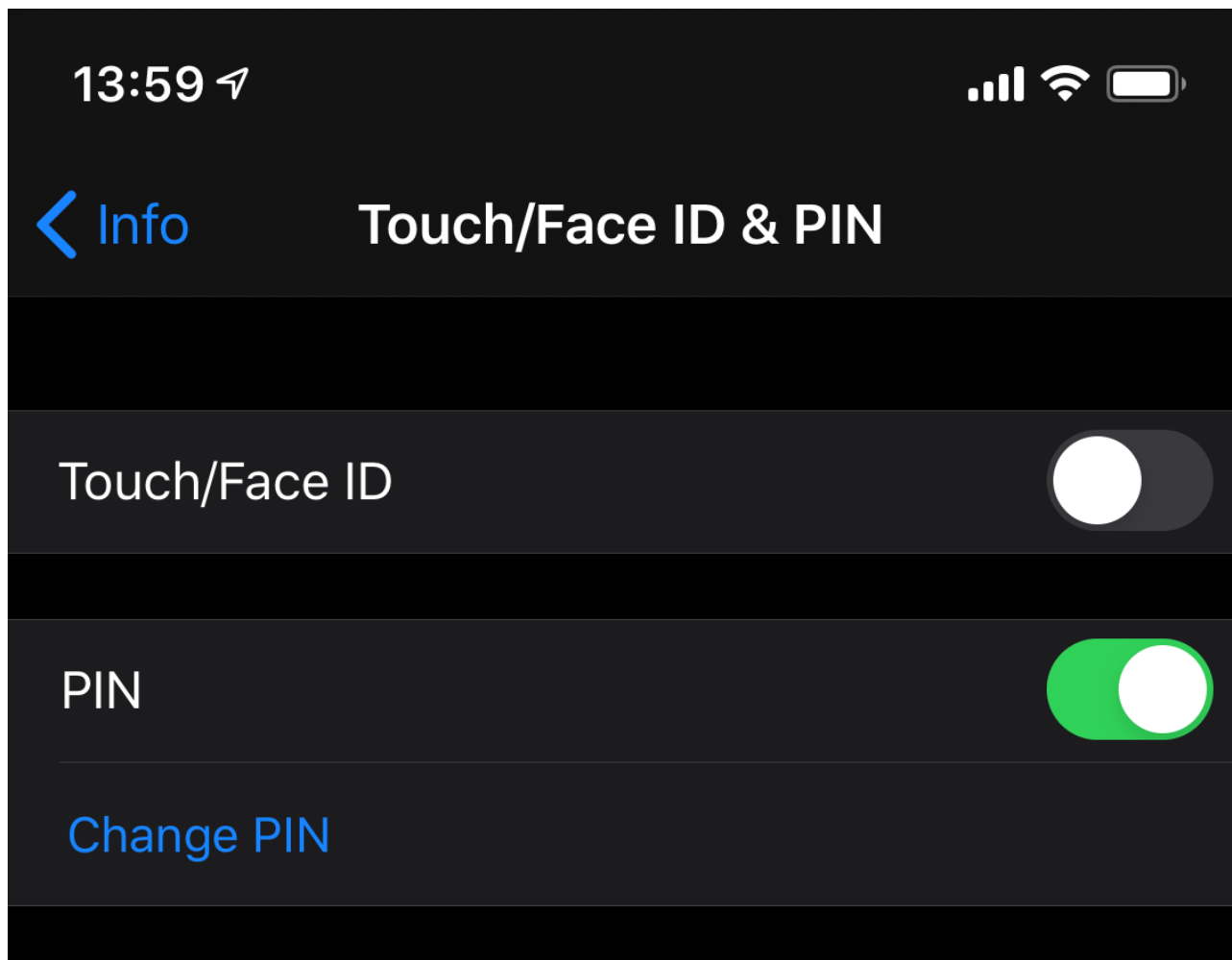
1. Open the FortiToken application and tap on *Info*.

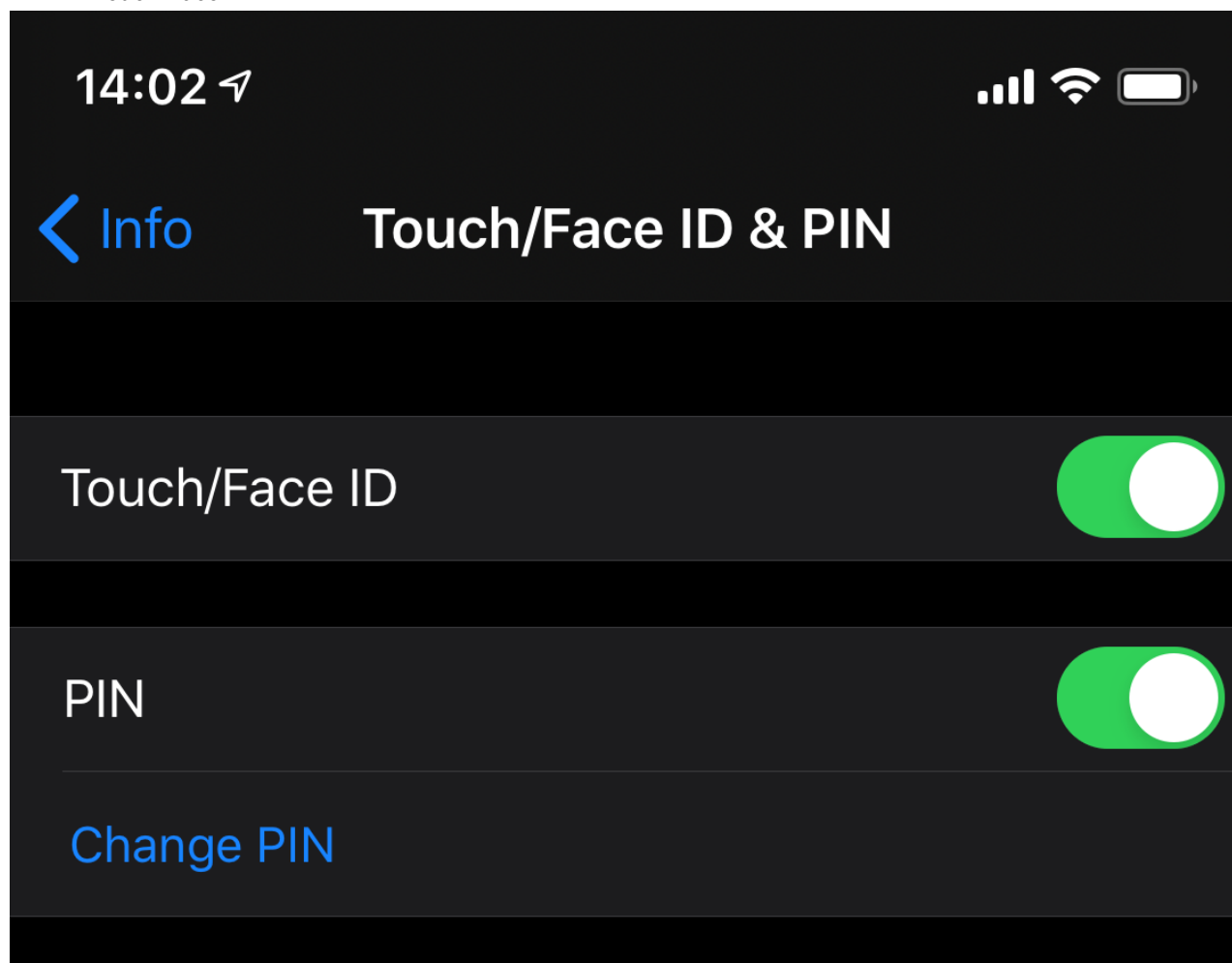


2. Tap on *Touch/Face ID & PIN*.



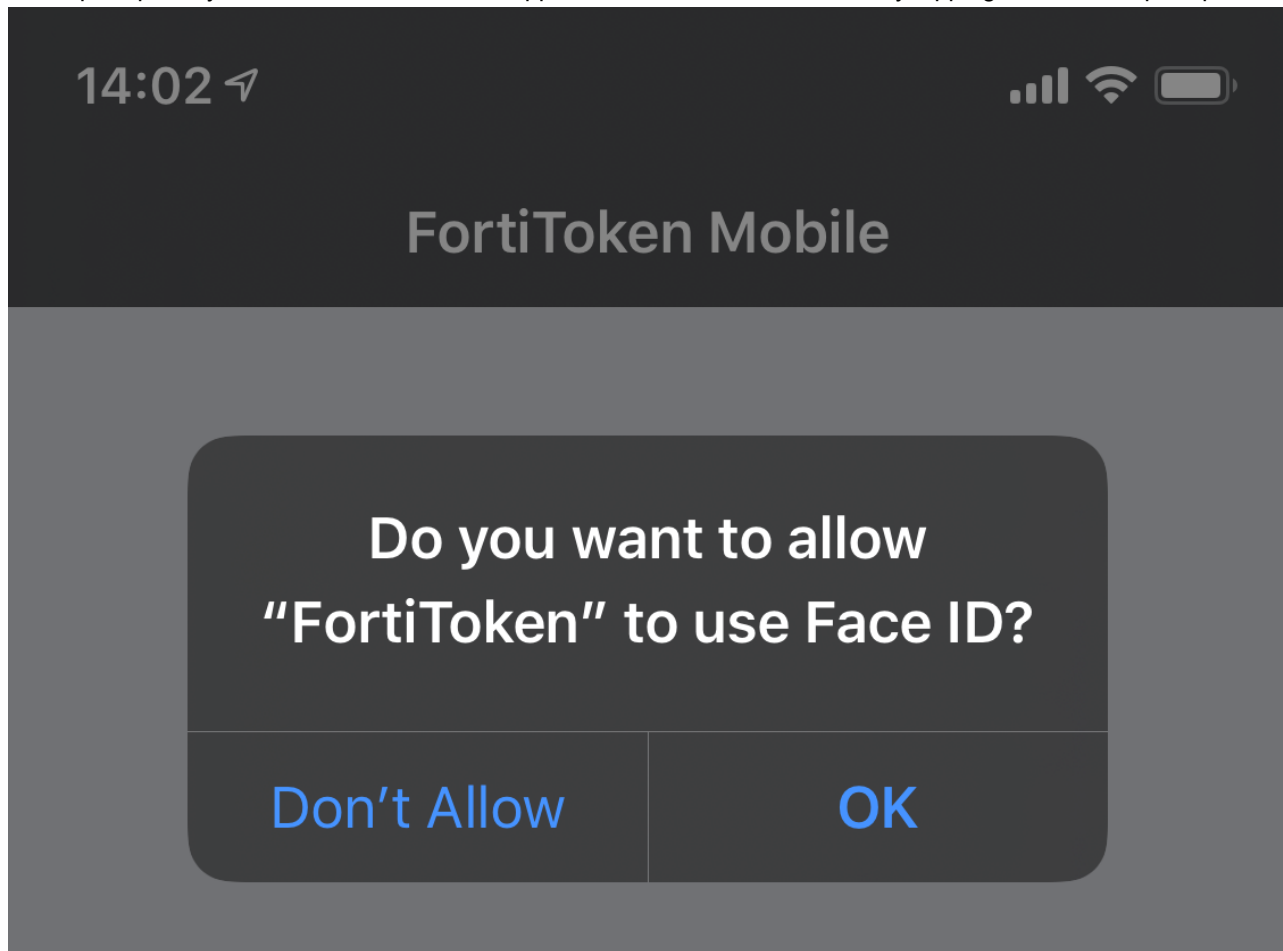
3. Enable and set up a 4-digit *PIN* for the application. The *PIN* is required to be enabled before you can enable *Touch/Face ID*.



4. Enable *Touch/Face ID*.

You cannot enable *Touch/Face ID* for FortiToken if *Touch/Face ID* is not set up and enabled for device unlock (*iPhone Unlock* in this case) on iOS. You must first set up and enable *Touch/Face ID* from *Settings* on your iOS device.

5. When prompted by iOS, allow the FortiToken application to use *Touch/Face ID* by tapping on *OK* in the prompt.



## Applying Multi-Factor Authentication

Multi-factor authentication may also be set up for SSL VPN users, administrators, firewall policy, wireless users, and so on. The following topics explain more about how you may use the newly created user in such scenarios:

- MFA for SSL VPN: [Set up FortiToken multi-factor authentication on page 1378](#)
- MFA for IPsec VPN: [Add FortiToken multi-factor authentication on page 1210](#)
- MFA for Administrators: [Associating a FortiToken to an administrator account on page 625](#)
- [MFA with Captive Portal](#)
- [MFA for wireless users via Captive Portal](#)
- [Configuring firewall authentication on page 1557](#)

## FortiToken Cloud

FortiToken Cloud is an Identity and Access Management as a Service (IDaaS) cloud service offering by Fortinet. It enables FortiGate and FortiAuthenticator customers to add MFA for their respective users, through the use of Mobile tokens or Hard tokens. It protects local and remote administrators as well as firewall and VPN users.

For information, see [Getting started—FGT-FTC users](#) in the [FortiToken Cloud Administration Guide](#).



## Registering hard tokens

Registering FortiTokens consists of the following steps:

1. [Adding FortiTokens to FortiOS.](#)
2. [Activating FortiTokens.](#)
3. [Associating FortiTokens with user accounts.](#)

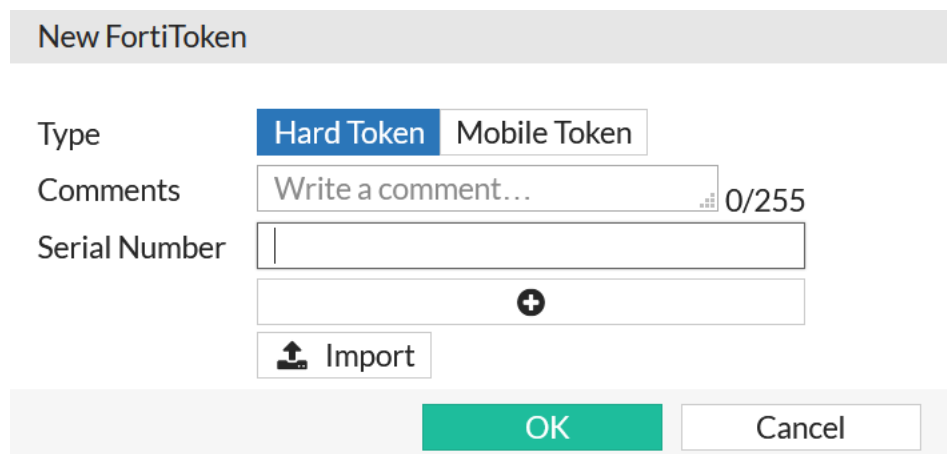
### Adding FortiTokens to FortiOS

You can add FortiTokens to FortiOS in the following ways:

- [Add FortiToken serial numbers using the GUI](#)
- [Add FortiToken serial numbers using the CLI](#)
- [Import FortiTokens using a serial number or seed file using the GUI](#)

**To manually add single hard token to FortiOS using the GUI:**

1. Go to *User & Device > FortiTokens*.
2. Click *Create New*.
3. For *Type*, select *Hard Token*.
4. In the *Serial Number* field, enter one or more FortiToken serial numbers.
5. Click *OK*.



New FortiToken

Type: **Hard Token** | Mobile Token

Comments: Write a comment... 0/255

Serial Number: [Empty field]

[+]

[Import]

OK | Cancel

**To add multiple FortiTokens to FortiOS using the CLI:**

```
config user fortitoken
 edit <serial_number>
 next
 edit <serial_number2>
 next
end
```

**To import multiple FortiTokens to FortiOS using the GUI:**

1. Go to *User & Device > FortiTokens*.
2. Click *Create New*.

3. For *Type*, select *Hard Token*.
4. Click *Import*. The *Import Tokens* section slides in on the screen.

5. Select *Serial Number File*.



Seed files are only used with FortiToken-200CD. These are special hardware tokens that come with FortiToken seeds on a CD. See the [FortiToken Comprehensive Guide](#) for details.

6. Click *Upload*.
7. Browse to the file's location on your local machine, select the file, then click *OK*.
8. Click *OK*.

## Activating FortiTokens

You must activate the FortiTokens before starting to use them. FortiOS requires connection to FortiGuard servers for FortiToken activation. During activation, FortiOS queries FortiGuard servers about each token's validity. Each token can only be used on a single FortiGate or FortiAuthenticator. If tokens are already registered, they are deemed invalid for re-activation on another device. FortiOS encrypts the serial number and information before sending for added security.

### To activate a FortiToken using the GUI:

1. Go to *User & Device > FortiTokens*.
2. Select the desired FortiTokens that have an *Available* status.
3. Click *Activate* from the menu above.
4. Click *Refresh*. The selected FortiTokens are activated.

### To activate a FortiToken using the CLI:

```
config user fortitoken
 edit <token_serial_num>
 set status activate
 next
end
```

## Associating FortiTokens with user accounts

You can associate FortiTokens with local user or administrator accounts.

### To associate a FortiToken to a local user account using the GUI:

1. Ensure that you have successfully added your FortiToken serial number to FortiOS and that its status is *Available*.
2. Go to *User & Device > User Definition*. Edit the desired user account.
3. In the *Email Address* field, enter the user's email address.
4. Enable *Two-factor Authentication*.
5. From the *Token* dropdown list, select the desired FortiToken serial number.
6. Click *OK*.

### To associate a FortiToken to a local user account using the CLI:

```
config user local
 edit <username>
 set type password
 set passwd "myPassword"
 set two-factor fortitoken
 set fortitoken <serial_number>
 set email-to "username@example.com"
 set status enable
 next
end
```



Before you can use a new FortiToken, you may need to synchronize it due to clock drift.

---

To associate a FortiToken to an administrator account, refer to the [Associating a FortiToken to an administrator account on page 625](#) section.

## Managing FortiTokens

This section focuses on the following:

- [Resending an activation email on page 1549](#)
- [Locking/unlocking FortiTokens on page 1550](#)
- [Managing FortiTokens drift on page 1550](#)
- [Deactivating FortiTokens on page 1551](#)
- [Moving FortiTokens to another device on page 1551](#)

### Resending an activation email

#### To resend an activation email/SMS for a mobile token on a FortiGate:

1. Go to *User & Device > User Definition*.
2. Double-click on the user to edit.

3. Click *Send Activation Code Email* from the *Two-factor Authentication* section.

## Locking/unlocking FortiTokens

### To change FortiToken status to active or to lock using the CLI:

```
config user fortitoken
 edit <token_serial_num>
 set status <active | lock>
 next
end
```

A user attempting to log in using a locked FortiToken cannot successfully authenticate.

Managing drift

## Managing FortiTokens drift

**If the FortiToken has drifted, the following must take place for the FortiToken to resynchronize with FortiOS:**

1. FortiOS prompts the user to enter a second code to confirm.
2. The user gets the next code from the FortiToken. They enter the code at the prompt.
3. FortiOS uses both codes to update its clock to match the FortiToken.

If you still experience clock drift, it may be the result of incorrect time settings on your mobile device. If so, make sure that the mobile device clock is accurate by confirming the network time and the correct timezone.

If the device clock is set correctly, the issue could be the result of the FortiGate and FortiTokens being initialized prior to setting an NTP server. This will result in a time difference that is too large to correct with the synchronize function. To avoid this, selected Tokens can be manually drift adjusted.

### To show current drift and status for each FortiToken from the CLI:

```
diagnose fortitoken info
FORTITOKEN DRIFT STATUS
FTK200XXXXXXXXXC 0 token already activated, and seed won't be returned
FTK200XXXXXXXXXE 0 token already activated, and seed won't be returned
FTKMOBXXXXXXXXXA 0 provisioned
FTKMOBXXXXXXXXX4 0 new
Total activated token: 0
Total global activated token: 0
Token server status: reachable
```

This command lists the serial number and drift for each configured FortiToken. You can check if it is necessary to synchronize the FortiGate and any particular FortiTokens.

### To adjust Mobile FortiToken for drift from the CLI:

```
exec fortitoken sync <FortiToken_ID> <token_code1> <next_token_code2>
```

## Deactivating FortiTokens

### To deactivate FortiToken on a FortiGate:

1. Go to *User & Device > User Definition*.
2. Select and edit the user for which you want to deactivate the token.
3. Disable the *Two-factor Authentication* toggle.
4. Click **OK**. The token will be removed from the user's *Two-factor Authentication* column. The user will also be removed from the token's *User* column under *User & Device > FortiTokens*.

## Moving FortiTokens to another device

FortiTokens can only be activated on a single FortiGate or FortiAuthenticator. To move FortiTokens to another device, you would first have to reset the registered FortiTokens on a device and then reactivate them on another device.

To reset Hard tokens registered to a FortiGate appliance (non-VM model), you can reset all hardware FTK200 tokens from the [Support Portal](#), or during RMA transfer. See the [Migrating users and FortiTokens to another FortiGate](#) KB article, for more information.



The above process will reset all Hard tokens and you cannot select individual tokens to reset.

---

To reset FortiToken Mobile, a single Hard token, a Hard token registered to a VM, and so on, an administrator must contact Customer Support and/or open a ticket on the [Support Portal](#).

Once reset, the FortiTokens can be activated on another FortiGate or FortiAuthenticator.

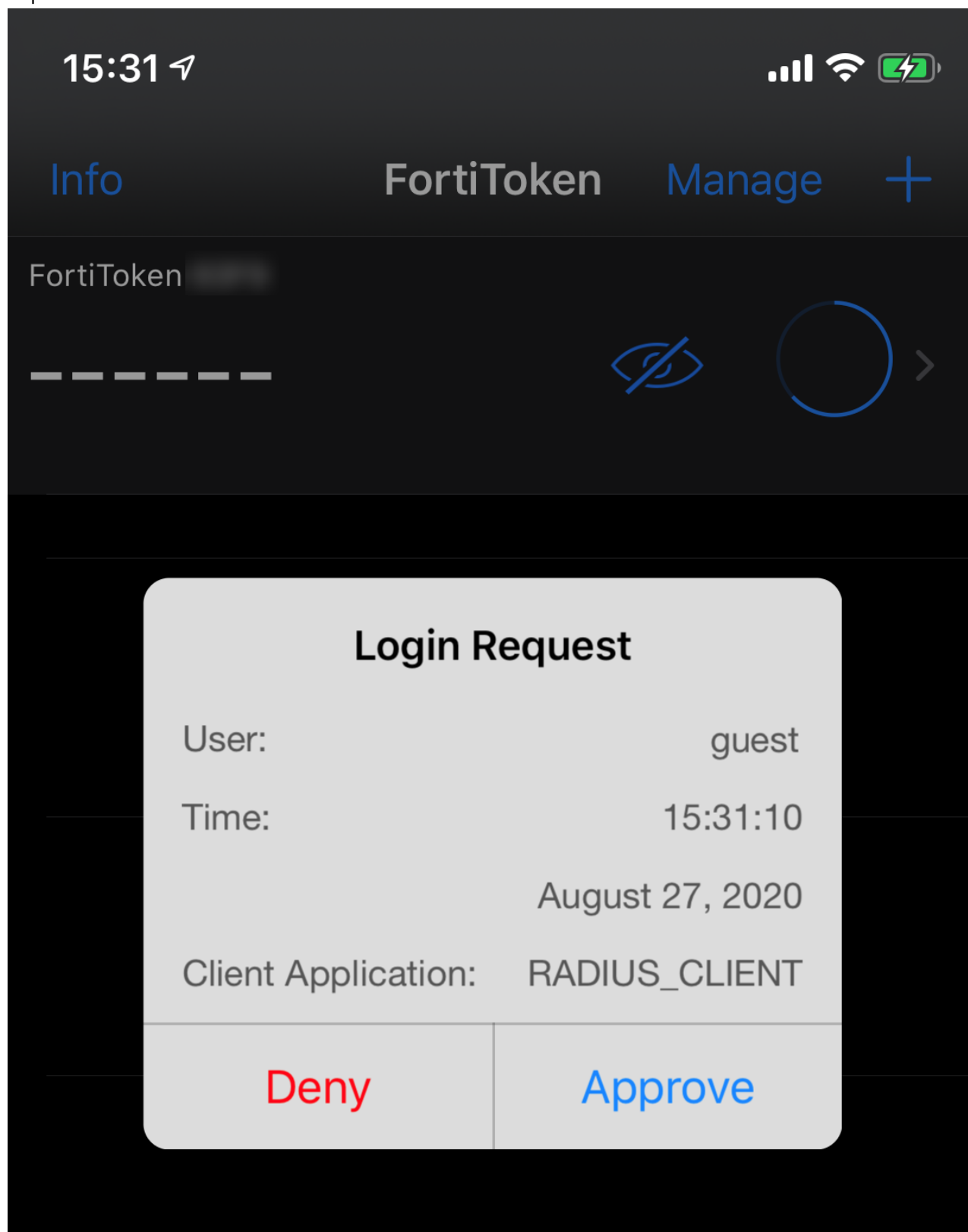
## FortiToken Mobile Push

FortiToken Mobile Push allows authentication requests to be sent as push notifications to the end user's FortiToken Mobile application.

The FortiToken Mobile push service operates as follows:

1. FortiGate sends a notification request by making a TLS connection with either Apple (for iOS) or Google (for Android) notification servers. Notification data may include the recipient, session, FortiGate callback IP and port, and so on.
2. The notification service from either Apple or Google notifies the user's mobile device of the push request.
3. The FortiToken Mobile application on the user's mobile displays a prompt for the user to either *Approve* or *Deny* the

request.



### To configure FortiToken Mobile push services using the CLI:

```
config system ftm-push
 set status enable
 set server-ip <ip-address>
 set server-port [1-65535]
end
```

The default server port is 4433.

The server IP address is the public IP address of the FortiOS interface that FortiToken Mobile calls back to. FortiOS uses this IP address for incoming FortiToken Mobile calls.

If an SSL VPN user authenticates with their token, then logs out and attempts to reauthenticate within a minute, a *Please wait x seconds to login again* message displays. This replaces a previous error/permission denied message. The x value depends on the calculation of how much time is left in the current time step.

```
config system interface
 edit "guest"
 set allowaccess ftm
 next
end
```



FortiOS supports FortiAuthenticator-initiated FortiToken Mobile Push notifications for users attempting to authenticate through an SSL VPN and/or RADIUS server (with FortiAuthenticator as the RADIUS server).

---

## Troubleshooting and diagnosis

This section contains some common scenarios for FortiTokens troubleshooting and diagnosis:

- [FortiToken Statuses on page 1553](#)
- [Recovering trial FortiTokens on page 1554](#)
- [Recovering lost Administrator FortiTokens on page 1555](#)
- [SSL VPN with multi-factor authentication expiry timers on page 1556](#)

### FortiToken Statuses

When troubleshooting FortiToken issues, it is important to understand different FortiToken statuses. FortiToken status may be retrieved either from the CLI or the GUI, with a slightly different naming convention.

Before you begin, verify that the FortiGate has Internet connectivity and is also connected to both the FortiGuard and registration servers:

```
exec ping fds1.fortinet.com
exec ping directregistration.fortinet.com
exec ping globalftm.fortinet.net
```



The `globalftm.fortinet.net` server is the Fortinet Anycast server added in FortiOS 6.4.2.

---

If there are connectivity issues, retrieving FortiToken statuses or performing FortiToken activation could fail. Therefore, troubleshoot connectivity issues before continuing.

### To retrieve FortiToken statuses:

- From the CLI:  
# diagnose fortitoken info
- From the GUI:  
Go to *User & Authentication > FortiTokens*.

Various FortiToken statuses in either the CLI or the GUI may be described as follows:

CLI	GUI	Description
new	<i>Available</i>	Newly added, not pending, not activated, not yet assigned.
active	<i>Assigned</i>	Assigned to a user, hardware token.
provisioning	<i>Pending</i>	Assigned to a user and waiting for activation on the FortiToken Mobile app.
provisioned	<i>Assigned</i>	Assigned to user and activated on the FortiToken Mobile app.
provision timeout		Token provided to user but not activated on the FortiToken Mobile app. To fix, the token needs to be re-provisioned and activated in time.
token already activated, and seed won't be returned	<i>Error</i>	Token is locked by FortiGuard FDS. The hardware token was already activated on another device and locked by FDS.
locked		Either manually locked by an Administrator ( <code>set status lock</code> ), or locked automatically, for example, when the token is unassigned and the FortiCare FTM provisioning server was unreachable to process that change.

## Recovering trial FortiTokens

You can recover trial FortiTokens if deleted from a FortiGate, or if stuck in a state where it is not possible to provision to a user.

When a token is stuck in an unusual state or with errors, delete the FortiTokens from the unit and proceed to recover trial FortiTokens.

### To recover trial tokens via the GUI:

1. Go to *User & Authentication > FortiTokens*.
2. Click the *Import Free Trial Tokens* button at the top. The two free trial tokens are recovered.

### To recover trial tokens via the CLI:

```
execute fortitoken-mobile import 0000-0000-0000-0000-0000
```



- Before attempting to recover the trial tokens, both the tokens should be deleted from the unit first.
- If VDOMs are enabled, trial tokens are in the management VDOM (`root` by default).



### Following error codes might come up in the CLI:

- If the device is not registered:  

```
exec fortitoken-mobile import 0000-0000-0000-0000-0000
import fortitoken license error: -7571
```
- If the serial number format is incorrect:  

```
exec fortitoken-mobile import 0000-0000-0000-0000-00
import fortitoken license error: -7566
```

### Recovering lost Administrator FortiTokens

If an Administrator loses their FortiToken or the FortiToken is not working, they will not be able to log into the admin console through the GUI or the CLI. If there is another Administrator that can log into the device, they may be able to reset the two-factor settings configured for the first Administrator, or create a new Admin user for them. Note that a *super\_admin* user will be able to edit other admin user settings, but a *prof\_admin* user will not be able to edit *super\_admin* settings.

In the case where there are no other administrators configured, the only option is to flash format the device and reload a backup config file. You must have console access to the device in order to format and flash the device. It is recommended to be physically on site to perform this operation.



The process of resetting an Admin user password using the maintainer account cannot be used to reset or disable two-factor authentication.

Before formatting the device, verify that you have a backup config file. You may or may not have the latest config file backed up, though you should consider using a backed up config file, and reconfigure the rest of the recent changes manually. Otherwise, you may need to configure your device starting from the default factory settings.

### To recover lost Administrator FortiTokens:

1. If you have a backed up config file:
  - a. Open the config file and search for the specific admin user. For representational purposes we will use `Test` in our example.

```
edit "Test"
 set accprofile "super_admin"
 set vdom "root"
 set two-factor fortitoken
 set fortitoken "FTKXXXXXXXXXX"
 set email-to "admin@email.com"
 set password ENC
 SH2BsE7VSvHKynpoY1nOupdfaefe/n+JaPrCMPFADY2U5kLUPnZwuitOpNz35YI=
 next
end
```

- b. Once you find the settings for the `Test` user, delete the fortitoken-related settings:

```
edit "Test"
 set accprofile "super_admin"
 set vdom "root"
 set password ENC
 SH2BsE7VSvHKynpoY1nOupdfaefe/n+JaPrCMPFADY2U5kLUPnZwuitOpNz35YI=
 next
end
```

2. Format the boot device during a maintenance window and reload the firmware image using instructions in the [Formatting and loading FortiGate firmware image using TFTP](#) KB article.
3. Once the reload is complete, log into the admin console from the GUI using the default admin user credentials, and go to *Configuration > Restore* from the top right corner to reload your config file created in Step 1 above.
4. Once the FortiGate reboots and your configuration is restored, you can log in with your admin user credentials.

## SSL VPN with multi-factor authentication expiry timers

When SSL VPN is configured with multi-factor authentication (MFA), sometimes you may require a longer token expiry time than the default 60 seconds.

### To configure token expiry timers using the CLI:

```
config system global
 set two-factor-ftk-expiry <number of seconds>
 set two-factor-ftm-expiry <number of seconds>
 set two-factor-sms-expiry <number of seconds>
 set two-factor-fac-expiry <number of seconds>
 set two-factor-email-expiry <number of seconds>
end
```

These timers apply to the tokens themselves and remain valid for as long as configured above. However, SSL VPN does not necessarily accept tokens for the entire duration they are valid. To ensure SSLVPN accepts the token for longer durations, you need to configure the remote authentication timeout setting accordingly.

### To configure the remote authentication timeout:

```
config system global
 set remoteauthtimeout <1-300 seconds>
end
```

SSL VPN waits for a maximum of five minutes for a valid token code to be provided before closing down the connection, even if the token code is valid for longer.



The `remoteauthtimeout` setting shows how long SSL VPN waits not only for a valid token to be provided before closing down the connection, but also for other remote authentication like LDAP, RADIUS, and so on.

---

## Configuring the maximum log in attempts and lockout period

Failed log in attempts can indicate malicious attempts to gain access to your network. To prevent this security risk, you can limit the number of failed log in attempts. After the configured maximum number of failed log in attempts is reached, access to the account is blocked for the configured lockout period.

### To configure number of maximum log in attempts:

This example sets the maximum number of log in attempts to five.

```
config user setting
 set auth-lockout-threshold 5
```

```
end
```

**To configure the lockout period in seconds:**

This example sets the lockout period to five minutes (300 seconds).

```
config user setting
 set auth-lockout-duration 300
end
```

## Creating a PKI/peer user

A PKI/peer user is a digital certificate holder. A FortiOS PKI user account contains the information required to determine which CA certificate to use to validate the user's certificate. You can include a peer user in a firewall user group or peer certificate group used in IPsec VPN.

To define a peer user, you need the following:

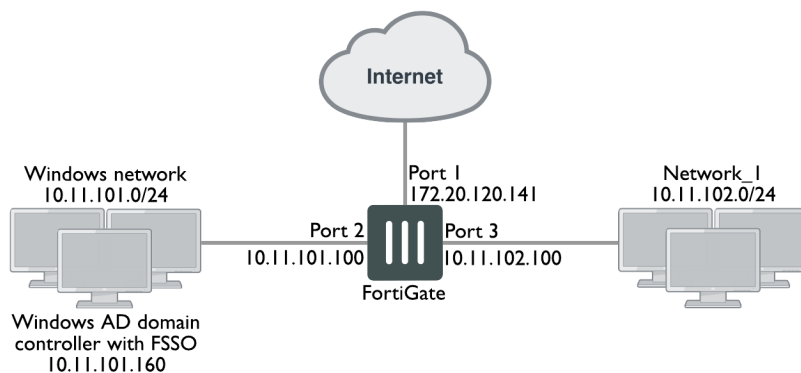
- Peer username
- Text from the user's certificate's subject field, or the name of the CA certificate used to validate the user's certificate

**To create a peer user for PKI authentication:**

```
config user peer
 edit peer1
 set subject peer1@mail.example.com
 set ca CA_Cert_1
 next
end
```

You can add or modify other configuration settings for PKI authentication, including configuring using an LDAP server to check client certificate access rights. See the [FortiOS CLI Reference](#).

## Configuring firewall authentication



In this example, a Windows network is connected to the FortiGate on port 2, and another LAN, Network\_1, is connected on port 3.

All Windows network users authenticate when they log on to their network. Engineering and Sales groups members can access the Internet without reentering their authentication credentials. The example assumes that you have already installed and configured FSSO on the domain controller.

LAN users who belong to the Internet\_users group can access the Internet after entering their username and password. The example shows two users: User1, authenticated by a password stored in FortiOS; and User 2, authenticated on an external authentication server. Both users are local users since you create the user accounts in FortiOS.

1. [Create a locally authenticated user account.](#)
2. [Create a RADIUS-authenticated user account.](#)
3. [Create an FSSO user group.](#)
4. [Create a firewall user group.](#)
5. [Define policy addresses.](#)
6. [Create security policies.](#)

## Creating a locally authenticated user account

User1 is authenticated by a password stored in FortiOS.

**To create a locally authenticated user account in the GUI:**

1. Go to *User & Device > User Definition*. Click *Create New*.
2. Configure the following settings:

Setting	Configuration
User Type	Local User
User Name	User1
Password	hardtoguess1@@1
User Account Status	Enabled

3. Click *Submit*.

**To create a locally authenticated user account in the CLI:**

```
config user local
edit user1
 set type password
 set passwd hardtoguess1@@1
next
end
```

## Creating a RADIUS-authenticated user account

You must first configure FortiOS to access the external authentication server, then create the user account.

**To create a RADIUS-authenticated user account in the GUI:**

1. Go to *User & Device > RADIUS Servers*. Click *Create New*.
2. Configure the following settings:

Setting	Configuration
Name	OurRADIUSsrv
Authentication method	Default
<b>Primary Server</b>	
IP/Name	10.11.101.15
Secret	OurSecret

3. Click *OK*.
4. Go to *User & Device > User Definition*. Click *Create New*.
5. Configure the following settings:

Setting	Configuration
User Type	Remote RADIUS User
User Name	User2
RADIUS Server	OurRADIUSsrv
User Account Status	Enabled

6. Click *Submit*.

**To create a RADIUS-authenticated user account in the CLI:**

```
config user radius
edit OurRADIUSsrv
 set server 10.11.102.15
 set secret OurSecret
 set auth-type auto
next
end
config user local
edit User2
 set name User2
 set type radius
 set radius-server OurRADIUSsrv
next
end
```

## Creating an FSSO user group

This example assumes that you have already set up FSSO on the Windows network and that it used advanced mode, meaning that it uses LDAP to access user group information. You must do the following:

- Configure LDAP access to the Windows AD global catalog
- Specify the collector agent that sends user logon information to FortiOS
- Select Windows user groups to monitor
- Select and add the Engineering and Sales groups to an FSSO user group

**To create an FSSO user group in the GUI:**

1. Configure LDAP for FSSO:
  - a. Go to *User & Device > LDAP Servers*. Click *Create New*.
  - b. Configure the following settings:

Setting	Configuration
Name	ADserver
Server Name / IP	10.11.101.160
Distinguished Name	dc=office,dc=example,dc=com
Bind Type	Regular
Username	cn=FSSO_Admin,cn=users,dc=office,dc=example,dc=com
Password	Enter a secure password.

- c. Leave other fields as-is. Click *OK*.
2. Specify the collector agent for FSSO;
    - a. Go to *Security Fabric > Fabric Connectors*. Click *Create New*.
    - b. Under *SSO/Identity*, select *Fortinet Single Sign-On Agent*.

## c. Configure the following settings:

Setting	Configuration
Name	Enter the Windows AD server name. This name appears in the Windows AD server list when you create user groups. In this example, the name is WinGroups.
Server IP/Name	Enter the IP address or name of the server where the agent is installed. The maximum name length is 63 characters. In this example, the IP address is 10.11.101.160.
Password	Enter the password of the server where the agent is installed. You only need to enter a password for the collector agent if you configured the agent to require authenticated access.  If the TCP port used for FSSO is not the default, 8000, you can run the <code>config user fsso</code> command to change the setting in the CLI.
Collector Agent AD access mode	Advanced
LDAP Server	Select the previously configured LDAP server. In this example, it is ADserver.
User/Groups/Organization Units	Select the users, groups, and OUs to monitor.

## d. Click OK.

## 3. Create the FSSO\_Internet\_users user group:

- a. Go to *User & Device > User Groups*. Click *Create New*.
- b. Configure the following settings:

Setting	Configuration
Name	FSSO_Internet_users
Type	Fortinet Single Sign-On (FSSO)
Members	Engineering, Sales

## c. Click OK.

**To create an FSSO user group in the CLI:**

```

config user ldap
 edit "ADserver"
 set server "10.11.101.160"
 set dn "cn=users,dc=office,dc=example,dc=com"
 set type regular
 set username "cn=administrator,cn=users,dc=office,dc=example,dc=com"
 set password set_a_secure_password
 next
end
config user fsso
 edit "WinGroups"
 set ldap-server "ADserver"
 set password *****

```

```
 set server "10.11.101.160"
 next
end
config user group
 edit FSSO_Internet_users
 set group-type fsso-service
 set member CN=Engineering,cn=users,dc=office,dc=example,dc=com
 CN=Sales,cn=users,dc=office,dc=example,dc=com
 next
end
```

## Creating a firewall user group

This example shows a firewall user group with only two users. You can add additional members.

### To create a firewall user group in the GUI:

1. Go to *User & Device > User Groups*. Click *Create New*.
2. Configure the following settings:

Setting	Configuration
Name	Internet_users
Type	Firewall
Members	User1, User2

3. Click OK.

### To create a firewall user group in the CLI:

```
config user group
 edit Internet_users
 set group-type firewall
 set member User1 User2
 next
end
```

## Defining policy addresses

### To define policy addresses:

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address*.
3. Configure the following settings:

Setting	Configuration
Name	Internal_net



Setting	Configuration
Type	Subnet
IP/Netmask	10.11.102.0/24
Interface	Port 3

4. Click *OK*.
5. Create another new address by repeating steps 2-4 using the following settings:

Setting	Configuration
Name	Windows_net
Type	Subnet
IP/Netmask	10.11.101.0/24
Interface	Port 2

## Creating security policies

You must create two security policies: one for the firewall group connecting through port 3, and one for the FSSO group connecting through port 2.

### To create security policies using the GUI:

1. Go to *Policy & Objects > IPv4 Policy*.
2. Click *Create New*.
3. Configure the following settings:

Setting	Configuration
Incoming Interface	Port2
Source Address	Windows_net
Source User(s)	FSSO_Internet_users
Outgoing Interface	Port1
Destination Address	all
Schedule	always
Service	ALL
NAT	Enabled.
Security Profiles	You can enable security profiles as desired.

4. Click *OK*.

5. Create another new policy by repeating steps 2-4 using the following settings:

Setting	Configuration
Incoming Interface	Port3
Source Address	Internal_net
Source User(s)	Internet_users
Outgoing Interface	Port1
Destination Address	all
Schedule	always
Service	ALL
NAT	Enabled.
Security Profiles	You can enable security profiles as desired.

6. Click OK.

#### To create security policies using the CLI:

```
config firewall policy
 edit 0
 set srcintf port2
 set dstintf port1
 set srcaddr Windows_net
 set dstaddr all
 set action accept
 set groups FSSO_Internet_users
 set schedule always
 set service ANY
 set nat enable
 next
end
config firewall policy
 edit 0
 set srcintf port3
 set dstintf port1
 set srcaddr internal_net
 set dstaddr all
 set action accept
 set schedule always
 set groups Internet_users
 set service ANY
 set nat enable
 next
end
```

# Wireless configuration

See the [FortiWiFi and FortiAP Cookbook](#).

# Switch Controller

Use the Switch Controller function, also known as FortiLink, to remotely manage FortiSwitch units. In the commonly-used layer 2 scenario, the FortiGate that is acting as a switch controller is connected to distribution FortiSwitch units. The distribution FortiSwitch units are in the top tier of stacks of FortiSwitch units and connected downwards with Convergent or Access layer FortiSwitch units. To leverage CAPWAP and the Fortinet proprietary FortiLink protocol, set up data and control planes between the FortiGate and FortiSwitch units.

FortiLink allows administrators to create and manage different VLANs, and apply the full-fledged security functions of FortiOS to them, such as 802.1X authentication and firewall policies. Most of the security control capabilities on the FortiGate are extended to the edge of the entire network, combining FortiGate, FortiSwitch, and FortiAP devices, and providing secure, seamless, and unified access control to users.

## FortiLink setup

Go to *WiFi & Switch Controller > FortiLink Interface* to create or edit FortiLink interfaces. The available options depend on the FortiGate model.

By automatically creating FortiLink interfaces as a logical aggregate or hard/soft switch, you can modify the FortiLink interfaces. If the physical port in use changes, you don't need to migrate existing policies.

## To configure FortiLink interfaces:

1. Go to *WiFi & Switch Controller > FortiLink Interface*.

2. Configure the interface settings and click *Apply*.

## FortiLink auto network configuration policy

The switch controller has a network `auto-config` option which contains configurable defaults, policy customization, and an individual interface override. This gives administrators simple and flexible control.

Following is a description of these options:

<code>auto-config default</code>	Provides the default actions for the first hop ( <code>fgt-policy</code> ) and lower-tier devices ( <code>isl-policy</code> ).
<code>auto-config policy</code>	A database containing policies that can be applied as a system-wide default or to a specific interface.
<code>auto-config custom</code>	Allows for the override of the <code>auto-config default</code> on a specific interface. This information is retained and is reapplied if an interface leaves and then is rediscovered.

**To configure automatic network detection:****1. Create or modify an auto-config policy:**

```

config switch-controller auto-config policy
 edit test123
 get
 name : test123
 qos-policy : default <== leverage the default qos-policy
 storm-control-policy: auto-config <== leverage auto-config storm-control-policy
 by default
 poe-status : enable <== If target of auto-config is poe port,
 keep poe-status enabled by default
 next
 end

```

**2. Designate an auto-config policy to FortiLink, ISL, or ICL on managed FortiSwitches.**

```

config switch-controller auto-config default
 get
 fgt-policy : test123
 isl-policy : test123
 icl-policy : test123
 set ?
 fgt-policy Default FortiLink auto-config policy.
 isl-policy Default ISL auto-config policy.
 icl-policy Default ICL auto-config policy.
 end

```

**3. Customize an auto-config policy for a specific FGT, ICL, or ISL interface.**

```

config switch-controller auto-config custom
 edit ?
 *name Auto-Config FortiLink or ISL/ICL interface name.
 edit G5H0E391790XXXX
 new entry 'G5H0E391790XXXX' added
 config switch-binding
 edit ?
 *switch-id Switch name.
 edit S524DN4K1500XXXX
 new entry 'S524DN4K1500XXXX' added
 get
 switch-id : S524DN4K1500XXXX
 policy : default
 next
 end
 next
 end
end

```

## FortiLink network sniffer extension

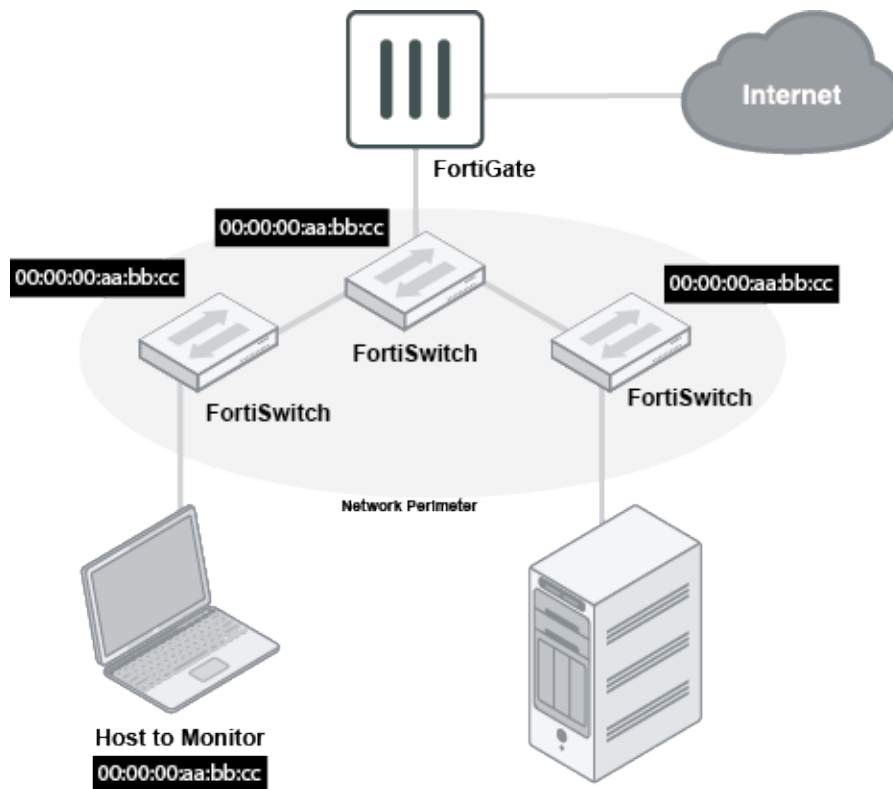
The switch controller has a `traffic-sniffer` option to provide a targeted approach where mirrored traffic is always directed towards the FortiGate on a dedicated VLAN. This allows for easy sniffing by using the CLI or GUI. Also, the traffic can be routed through the FortiGate using Encapsulated Remote Switched Port Analyzer (ERSPAN) for external analysis and storage.

Use this option to define targeted sniffers by IP or MAC address. Traffic matching is replicated to the FortiGate, which is helpful when you know what device you are looking for but don't know where it is located.

FortiLink networks can have multiple switches and traffic typically traverses several switches. If each switch mirrors any match, the sniffer would see multiple copies of traffic. To reduce this, the targets are applied at the perimeter of the FortiSwitch network. Traffic entering by a user port or traffic from FortiGate is considered eligible for mirroring.

You can also enable traditional port-based sniffers in the ingress or egress direction.

All sniffer traffic arrives at the FortiGate using ERSPAN and the traffic is encapsulated in generic routing encapsulation (GRE).



You can only configure this feature using the CLI.

#### To use predefined sniffer-used switch VLAN interface:

```
config system interface
 edit "snf.aggr1" <---- Newly added pre-defined switch vlan interface. Created
 automatically, once first FSW discovered and authorized.
 set vdom "root"
 set ip 10.254.253.254 255.255.254.0
 set allowaccess ping
 set description "Sniffer VLAN"
 set snmp-index 33
 set switch-controller-traffic-policy "sniffer"
 set color 6
 set interface "aggr1"
 set vlanid 4092
 next
 end
```

### To enable traffic sniffer based on target IP or MAC address on target ports of managed FortiSwitch units:

```
config switch-controller traffic-sniffer <---- newly added CLI stanza in FOS
 set erspan-ip 2.2.2.2 <---- Designate ERSPAN collector
 config target-mac
 edit 11:11:11:11:11:11
 next
 end
 config target-ip
 edit 4.4.4.4
 next
 end
 config target-port
 edit "S524DN4K1500XXXX"
 set in-ports "port2" "port4" "port6"
 set out-ports "port3" "port5" "port7"
 next
 end
end
```

### To use troubleshooting tools:

```
(root) # diagnose switch-controller switch-info mirror status S524DN4K1500XXXX
```

```
Managed Switch : S524DN4K1500XXXX
flink.sniffer
 Mode : ERSPAN-auto
 Status : Active
 Source-Ports:
 Ingress: port2, port4, port6
 Egress : port3, port5, port7
 Used-by-ACLs : True
 Auto-config-state : Resolved/Running
 Last-update : 1464 seconds ago
 Issues : None
 Collector-IP : 2.2.2.2
 Source-IP : 10.254.252.208
 Source-MAC : 08:5b:0e:ff:40:27
 Next-Hop :
 IP : 10.254.253.254
 MAC : 00:09:0f:09:00:0c
 Via-System-Interface : sniffer
 VLAN : 4092 (tagged)
 Via-Switch-Interface : G5H0E391790XXXX
```

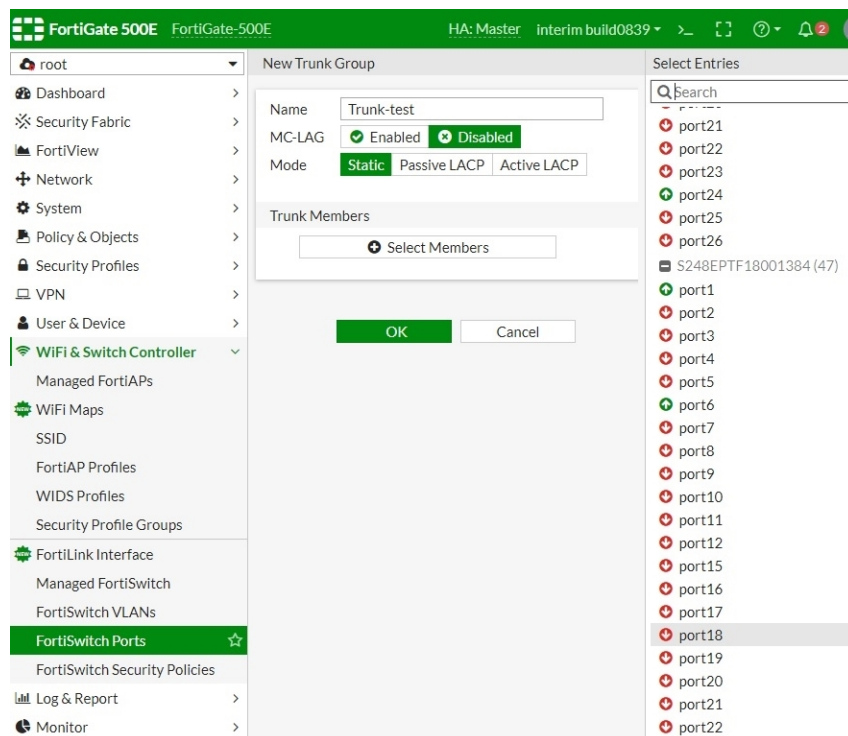
## FortiLink MCLAG configuration

In *WiFi & Switch Controller > FortiSwitch Ports*, you can enable MCLAG and view ports grouped by trunks. You need to configure ports from two switches, that is, two MCLAG peer switches to be included in one MCLAG.

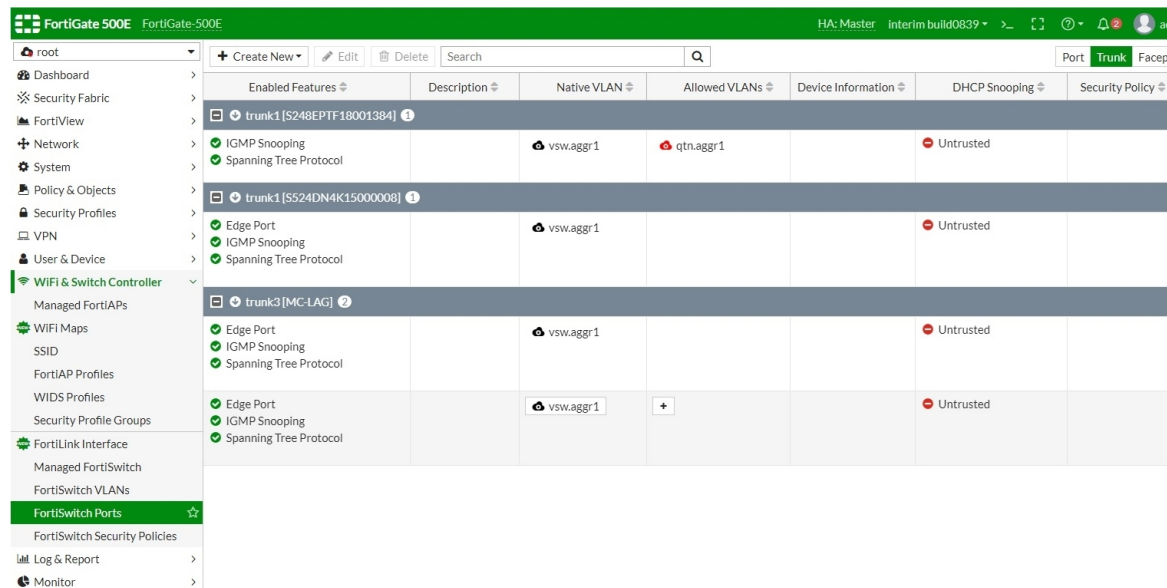


## Sample configuration

In *WiFi & Switch Controller > FortiSwitch Ports*, there is an *MC-LAG* option.



In *WiFi & Switch Controller > FortiSwitch Ports*, there is a *Trunk* view.



## Standalone FortiGate as switch controller

The following recipes provide instructions on configuring a standalone FortiGate as a switch controller:

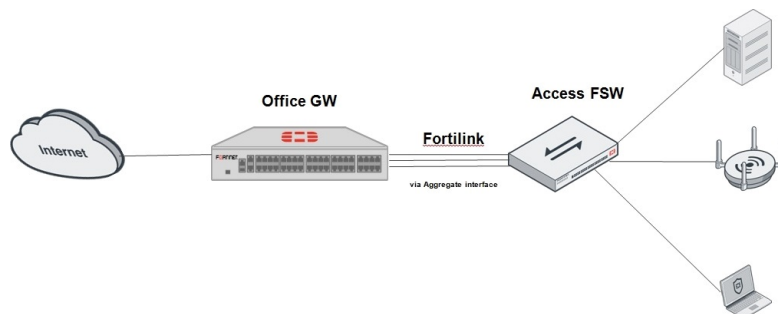
- [Standalone FortiGate as switch controller](#)
- [Multiple FortiSwitches managed via hardware/software switch on page 1575](#)
- [Multiple FortiSwitches in tiers via aggregate interface with redundant link enabled on page 1579](#)
- [Multiple FortiSwitches in tiers via aggregate interface with MCLAG enabled only on distribution on page 1582](#)

## Standalone FortiGate as switch controller

In this example, one FortiSwitch is managed by a standalone FortiGate. The FortiGate uses an aggregate interface to operate as a switch controller. This configuration might be used in branch office. It might also be used before increasing the number of connected FortiSwitch units and evolving to a multi-tier structure.

### Prerequisites:

- The FortiGate model supports an aggregate interface.
- FortiSwitch units have been upgraded to latest released software version.
- Layer-3 path/route in the management VDOM is available to Internet so that the FortiSwitch units can synchronize NTP.



### Change the FortiSwitch management mode to FortiLink:

Enter the following CLI commands on the FortiSwitch:

```

config system global
 set switch-mgmt-mode fortilink
end
This operation will cleanup all of the configuration and reboot the system!
Do you want to continue? (y/n)y
Backing up local mode config before entering FortiLink mode....

```

If the FortiSwitch ports used for the FortiLink connection have `auto-discovery-fortilink` enabled, executing authorization on FortiGate will trigger the transformation to FortiLink mode automatically.

```

config switch interface
 edit "port1"
 set auto-discovery-fortilink enable


```

```

 next
end

```

### Create an aggregate interface and designate it as Fortilink interface on the FortiGate:

Using the CLI:

```

config system interface
 edit "aggr1"
 set vdom "vdom1"
 set fortilink enable
 set type aggregate
 set member "port11" "port12"
 next
end

```

Using the GUI:

1. Go to *WiFi & Switch Controller > FortiLink Interface*.
2. In *Interface members*, select an existing aggregate interface (if there is one) or select one or more physical ports to create an aggregate interface.
3. Configure other fields as necessary.
4. Click **OK**.

### Discover and authorize the FortiSwitch:

Using the CLI:

```

config switch-controller managed-switch
 edit "FSWSerialNum"
 set fsw-wan1-admin enable

next
end

```

Check the CLI output for **Connection: Connected** to show that FortiLink is up:

```
execute switch-controller get-conn-status FSWSerialNum
```

```

Get managed-switch S248EPTF18001384 connection status:
Admin Status: Authorized
Connection: Connected
Image Version: S248EP-v6.2.0-build143,190107 (Interim)
Remote Address: 2.2.2.2
Join Time: Fri Jan 11 15:22:32 2019

```

interface	status	duplex	speed	fortilink	stacking	poe status
port1	up	full	1000Mbps	no	no	Delivering Power
port2	down	N/A	0	no	no	Searching
.....						

Using the GUI:

1. Go to *WiFi & Switch Controller > Managed FortiSwitch*.
2. Click **Authorize** and wait for a few minutes for the connection to be established.  
When FortiLink between the FortiGate and FortiSwitch is established, the Link-up ports change to green and the POE port that is supplying power changes to blue. The dotted line between the FortiGate and FortiSwitch changes

to a solid line. The Connection status shows that FortiLink is up.

### Extend the security perimeter to the edge of FortiSwitch:

1. Configure the VLAN arrangement.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch VLANs*.
  - b. Configure the VLAN interfaces that are applied on FortiSwitch.  
On FortiGate, these switch VLAN interfaces are treated as layer-3 interfaces and are available to be applied by firewall policy and other security controls in FortiOS. This means that security boundary is extended to FortiSwitch.
2. Configure FortiSwitch ports.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch Ports*.
  - b. Select one or more FortiSwitch ports and assign them to the switch VLAN.
  - c. You can also select *POE/DHCP Snooping*, *STP*, and other parameters for the FortiSwitch ports to show their real-time status such as link status, data statistics, etc.
3. Configure access authentication.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch Security Policies*.
  - b. Configure the *802.1X* security policies.
  - c. Select *Port-based* or *MAC-based* mode and select *User groups* from the existing VDOM.
  - d. Configure other fields as necessary.
  - e. Go to *WiFi & Switch Controller > FortiSwitch Ports*.
  - f. Select one or more FortiSwitch ports, click + in the *Security Policy* column, then make a selection from the pane.

## Troubleshooting

### Authorized FortiSwitch always offline

If an authorized FortiSwitch is always offline, go to the FortiGate CLI and use the command below to see all the checkpoints. Inspect each checkpoint to find the cause of the problem.

```
execute switch-controller diagnose-connection S248EPTF18001384

Fortilink interface ... OK
aggr1 enabled

DHCP server ... OK
aggr1 enabled

NTP server ... OK
aggr1 enabled
NTP server sync ... OK
synchronized: yes, ntpsync: enabled, server-mode: enabled

ipv4 server(ntp1.fortiguard.com) 208.91.113.70 -- reachable(0x80) S:2 T:128
no data
ipv4 server(ntp2.fortiguard.com) 208.91.113.71 -- reachable(0x80) S:2 T:128
no data
ipv4 server(ntp2.fortiguard.com) 208.91.112.51 -- reachable(0xff) S:2 T:66 selected
server-version=4, stratum=2
reference time is dfe3aec5.744404e6 -- UTC Sat Jan 12 00:09:41 2019
```

```
clock offset is -0.320411 sec, root delay is 0.054535 sec
root dispersion is 0.533081 sec, peer dispersion is 11495 msec

ipv4 server(ntp1.fortiguard.com) 208.91.112.50 -- reachable(0xff) S:2 T:66
server-version=4, stratum=2
reference time is dfe3aec5.744404e6 -- UTC Sat Jan 12 00:09:41 2019
clock offset is -0.448087 sec, root delay is 0.054535 sec
root dispersion is 0.533081 sec, peer dispersion is 12542 msec

HA mode ... disabled

Fortilink
Status ... SWITCH_AUTHORIZED_READY
Last keepalive ... 1 seconds ago

CAPWAP
Remote Address: 2.2.2.2
Status ... CONNECTED
Last keepalive ... 26 seconds ago

PING 2.2.2.2 (2.2.2.2): 56 data bytes
64 bytes from 2.2.2.2: icmp_seq=0 ttl=64 time=1.1 ms
64 bytes from 2.2.2.2: icmp_seq=1 ttl=64 time=13.9 ms
64 bytes from 2.2.2.2: icmp_seq=2 ttl=64 time=12.7 ms
64 bytes from 2.2.2.2: icmp_seq=3 ttl=64 time=2.9 ms
64 bytes from 2.2.2.2: icmp_seq=4 ttl=64 time=1.2 ms

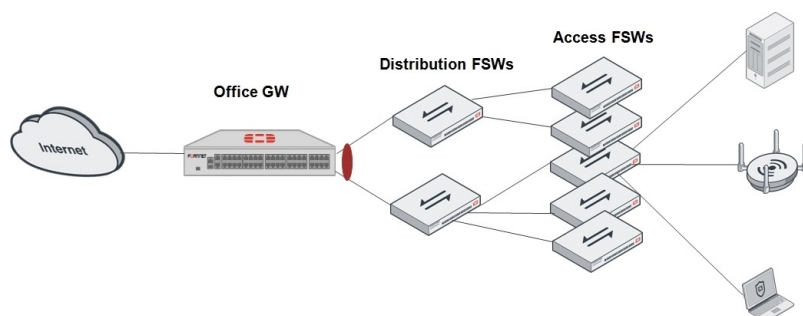
--- 2.2.2.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.1/6.3/13.9 ms
```

## Multiple FortiSwitches managed via hardware/software switch

This example provides a recommended configuration of FortiLink where multiple FortiSwitches are managed by a standalone FortiGate as switch controller via hardware or software switch interface; such as when you need multiple distribution FortiSwitches but lack supporting aggregate on FortiGate.

### Prerequisites:

- The FortiGate model supports hardware or software switch interface.
- FortiSwitch units have been upgraded to latest released software version.
- Layer-3 path/route in the management VDOM is available to Internet so that the FortiSwitch units can synchronize NTP.



**Change the FortiSwitch management mode to FortiLink:**

Enter the following CLI commands on the FortiSwitch:

```
config system global
 set switch-mgmt-mode fortilink
end
This operation will cleanup all of the configuration and reboot the system!
Do you want to continue? (y/n)y
Backing up local mode config before entering FortiLink mode....
```

If the FortiSwitch ports used for the FortiLink connection have `auto-discovery-fortilink` enabled, executing authorization on FortiGate will trigger the transformation to FortiLink mode automatically.

```
config switch interface
 edit "port1"
 set auto-discovery-fortilink enable

next
end
```

**Create hardware or software switch interface and designate it as FortiLink interface on the FortiGate:**

Create a hardware switch using the CLI:

```
config system virtual-switch
 edit "hardswitch1"
 set physical-switch "sw0"
 config port
 edit "port11"
 next
 edit "port12"
 next
 end
next
end
```

Create a software switch using the CLI:

```
config system switch-interface
 edit "softswitch1"
 set vdom "vdom1"
 set member "port11" "port12"
 next
end
```

Using the GUI:

1. Go to *WiFi & Switch Controller > FortiLink Interface*.
2. In *Interface members*, select an existing hardware/software switch interface (if there is one) or select one or more physical ports to create a hardware/software switch interface.
3. Configure other fields as necessary.
4. Click *OK*.

**Discover and authorize the FortiSwitch:**

Using the CLI:

```

config switch-controller managed-switch
 edit "FSWSerialNum"
 set fsw-wan1-admin enable

next
end

```

Check the CLI output for Connection: Connected to show that FortiLink is up:

```
execute switch-controller get-conn-status FSWSerialNum
```

```

Get managed-switch S248EPTF18001384 connection status:
Admin Status: Authorized
Connection: Connected
Image Version: S248EP-v6.2.0-build143,190107 (Interim)
Remote Address: 2.2.2.2
Join Time: Fri Jan 11 15:22:32 2019

```

interface	status	duplex	speed	fortilink	stacking	poe status
port1	up	full	1000Mbps	no	no	Delivering Power
port2	down	N/A	0	no	no	Searching
.....						

Using the GUI:

1. Go to *WiFi & Switch Controller > Managed FortiSwitch*.
2. Click *Authorize* and wait for a few minutes for the connection to be established.  
When FortiLink between the FortiGate and FortiSwitch is established, the Link-up ports change to green and the POE port that is supplying power changes to blue. The dotted line between the FortiGate and FortiSwitch changes to a solid line. The Connection status shows that FortiLink is up.

### Extend the security perimeter to the edge of FortiSwitch:

1. Configure the VLAN arrangement.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch VLANs*.
  - b. Configure the VLAN interfaces that are applied on FortiSwitch.  
On FortiGate, these switch VLAN interfaces are treated as layer-3 interfaces and are available to be applied by firewall policy and other security controls in FortiOS. This means that security boundary is extended to FortiSwitch.
2. Configure FortiSwitch ports.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch Ports*.
  - b. Select one or more FortiSwitch ports and assign them to the switch VLAN.
  - c. You can also select *POE/DHCP Snooping*, *STP*, and other parameters for the FortiSwitch ports to show their real-time status such as link status, data statistics, etc.
3. Configure access authentication.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch Security Policies*.
  - b. Configure the *802.1X* security policies.
  - c. Select *Port-based* or *MAC-based* mode and select *User groups* from the existing VDOM.
  - d. Configure other fields as necessary.
  - e. Go to *WiFi & Switch Controller > FortiSwitch Ports*.
  - f. Select one or more FortiSwitch ports, click + in the *Security Policy* column, then make a selection from the pane.

## Troubleshooting

### Bind FortiLink on hardware switch interface

Fortinet recommends binding FortiLink on the hardware switch interface. Since the hardware switch interface can leverage hardware chips to forward traffic, it does not consume CPU capacity, unlike a software switch.

### Authorized FortiSwitch always offline

If an authorized FortiSwitch is always offline, go to the FortiGate CLI and use the command below to see all the checkpoints. Inspect each checkpoint to find the cause of the problem.

```
execute switch-controller diagnose-connection S248EPTF18001384

Fortilink interface ... OK
hardswitch1 enabled

DHCP server ... OK
hardswitch1 enabled

NTP server ... OK
hardswitch1 enabled
NTP server sync ... OK
synchronized: yes, ntpsync: enabled, server-mode: enabled

ipv4 server(ntp1.fortiguard.com) 208.91.113.70 -- reachable(0x80) S:2 T:128
 no data
ipv4 server(ntp2.fortiguard.com) 208.91.113.71 -- reachable(0x80) S:2 T:128
 no data
ipv4 server(ntp2.fortiguard.com) 208.91.112.51 -- reachable(0xff) S:2 T:66 selected
 server-version=4, stratum=2
 reference time is dfe3aec5.744404e6 -- UTC Sat Jan 12 00:09:41 2019
 clock offset is -0.320411 sec, root delay is 0.054535 sec
 root dispersion is 0.533081 sec, peer dispersion is 11495 msec

ipv4 server(ntp1.fortiguard.com) 208.91.112.50 -- reachable(0xff) S:2 T:66
 server-version=4, stratum=2
 reference time is dfe3aec5.744404e6 -- UTC Sat Jan 12 00:09:41 2019
 clock offset is -0.448087 sec, root delay is 0.054535 sec
 root dispersion is 0.533081 sec, peer dispersion is 12542 msec

HA mode ... disabled

Fortilink
Status ... SWITCH_AUTHORIZED_READY
Last keepalive ... 1 seconds ago

CAPWAP
Remote Address: 2.2.2.2
Status ... CONNECTED
Last keepalive ... 26 seconds ago

PING 2.2.2.2 (2.2.2.2): 56 data bytes
64 bytes from 2.2.2.2: icmp_seq=0 ttl=64 time=1.1 ms
64 bytes from 2.2.2.2: icmp_seq=1 ttl=64 time=13.9 ms
64 bytes from 2.2.2.2: icmp_seq=2 ttl=64 time=12.7 ms
```



```

64 bytes from 2.2.2.2: icmp_seq=3 ttl=64 time=2.9 ms
64 bytes from 2.2.2.2: icmp_seq=4 ttl=64 time=1.2 ms

--- 2.2.2.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.1/6.3/13.9 ms

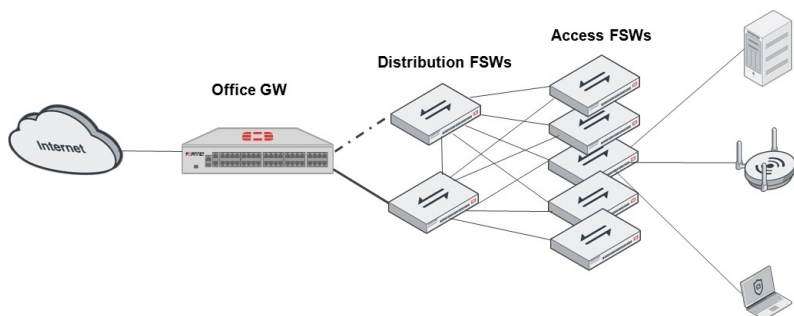
```

## Multiple FortiSwitches in tiers via aggregate interface with redundant link enabled

This example provides a recommended configuration of FortiLink where multi-tier FortiSwitches are managed by a standalone FortiGate as switch controller via aggregate interface, where the FortiGate can provide redundant links to multiple distribution FortiSwitches.

### Prerequisites:

- The FortiGate model supports an aggregate interface.
- FortiSwitch units have been upgraded to latest released software version.
- Layer-3 path/route in the management VDOM is available to Internet so that the FortiSwitch units can synchronize NTP.



### Change the FortiSwitch management mode to FortiLink:

Enter the following CLI commands on the FortiSwitch:

```

config system global
 set switch-mgmt-mode fortilink
end
This operation will cleanup all of the configuration and reboot the system!
Do you want to continue? (y/n)y
Backing up local mode config before entering FortiLink mode....

```

If the FortiSwitch ports used for the FortiLink connection have `auto-discovery-fortilink` enabled, executing authorization on FortiGate will trigger the transformation to FortiLink mode automatically.

```

config switch interface
 edit "port1"
 set auto-discovery-fortilink enable

next
end

```

## Create an aggregate interface and designate it as Fortilink interface on the FortiGate:

Using the CLI:

```
config system interface
 edit "aggr1"
 set vdom "vdom1"
 set fortilink enable
 set type aggregate
 set member "port11" "port12"
 set fortilink-split-interface enable
 next
end
```

Using the GUI:

1. Go to *WiFi & Switch Controller > FortiLink Interface*.
2. In *Interface members*, select one or more physical ports that are connected to different distribution FortiSwitches to create an aggregate interface.
3. Enable *FortiLink split interface*.
4. Configure other fields as necessary.
5. Click **OK**.

## Discover and authorize the FortiSwitch:

Using the CLI:

```
config switch-controller managed-switch
 edit "FSWSerialNum"
 set fsw-wan1-admin enable

next
end
```

Check the CLI output for Connection: Connected to show that FortiLink is up:

```
execute switch-controller get-conn-status FSWSerialNum
```

```
Get managed-switch S248EPTF18001384 connection status:
Admin Status: Authorized
Connection: Connected
Image Version: S248EP-v6.2.0-build143,190107 (Interim)
Remote Address: 2.2.2.2
Join Time: Fri Jan 11 15:22:32 2019
```

interface	status	duplex	speed	fortilink	stacking	poe status
port1	up	full	1000Mbps	no	no	Delivering Power
port2	down	N/A	0	no	no	Searching
.....						

Using the GUI:

1. Go to *WiFi & Switch Controller > Managed FortiSwitch*.
2. Click **Authorize** and wait for a few minutes for the connection to be established.  
When FortiLink between the FortiGate and FortiSwitch is established, the Link-up ports change to green and the POE port that is supplying power changes to blue. The dotted line between the FortiGate and FortiSwitch changes to a solid line. The Connection status shows that FortiLink is up.

## Extend the security perimeter to the edge of FortiSwitch:

1. Configure the VLAN arrangement.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch VLANs*.
  - b. Configure the VLAN interfaces that are applied on FortiSwitch.  
On FortiGate, these switch VLAN interfaces are treated as layer-3 interfaces and are available to be applied by firewall policy and other security controls in FortiOS. This means that security boundary is extended to FortiSwitch.
2. Configure FortiSwitch ports.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch Ports*.
  - b. Select one or more FortiSwitch ports and assign them to the switch VLAN.
  - c. You can also select *POE/DHCP Snooping*, *STP*, and other parameters for the FortiSwitch ports to show their real-time status such as link status, data statistics, etc.
3. Configure access authentication.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch Security Policies*.
  - b. Configure the *802.1X* security policies.
  - c. Select *Port-based* or *MAC-based* mode and select *User groups* from the existing VDOM.
  - d. Configure other fields as necessary.
  - e. Go to *WiFi & Switch Controller > FortiSwitch Ports*.
  - f. Select one or more FortiSwitch ports, click + in the *Security Policy* column, then make a selection from the pane.

## Troubleshooting

### Authorized FortiSwitch always offline

If an authorized FortiSwitch is always offline, go to the FortiGate CLI and use the command below to see all the checkpoints. Inspect each checkpoint to find the cause of the problem.

```
execute switch-controller diagnose-connection S248EPTF18001384

Fortilink interface ... OK
aggr1 enabled

DHCP server ... OK
aggr1 enabled

NTP server ... OK
aggr1 enabled
NTP server sync ... OK
synchronized: yes, ntpsync: enabled, server-mode: enabled

ipv4 server(ntp1.fortiguard.com) 208.91.113.70 -- reachable(0x80) S:2 T:128
no data
ipv4 server(ntp2.fortiguard.com) 208.91.113.71 -- reachable(0x80) S:2 T:128
no data
ipv4 server(ntp2.fortiguard.com) 208.91.112.51 -- reachable(0xff) S:2 T:66 selected
server-version=4, stratum=2
reference time is dfe3aec5.744404e6 -- UTC Sat Jan 12 00:09:41 2019
clock offset is -0.320411 sec, root delay is 0.054535 sec
root dispersion is 0.533081 sec, peer dispersion is 11495 msec
```

```
ipv4 server(ntpl.fortiguard.com) 208.91.112.50 -- reachable(0xff) S:2 T:66
 server-version=4, stratum=2
 reference time is dfe3aec5.744404e6 -- UTC Sat Jan 12 00:09:41 2019
 clock offset is -0.448087 sec, root delay is 0.054535 sec
 root dispersion is 0.533081 sec, peer dispersion is 12542 msec

HA mode ... disabled

Fortilink
Status ... SWITCH_AUTHORIZED_READY
Last keepalive ... 1 seconds ago

CAPWAP
Remote Address: 2.2.2.2
Status ... CONNECTED
Last keepalive ... 26 seconds ago

PING 2.2.2.2 (2.2.2.2): 56 data bytes
64 bytes from 2.2.2.2: icmp_seq=0 ttl=64 time=1.1 ms
64 bytes from 2.2.2.2: icmp_seq=1 ttl=64 time=13.9 ms
64 bytes from 2.2.2.2: icmp_seq=2 ttl=64 time=12.7 ms
64 bytes from 2.2.2.2: icmp_seq=3 ttl=64 time=2.9 ms
64 bytes from 2.2.2.2: icmp_seq=4 ttl=64 time=1.2 ms

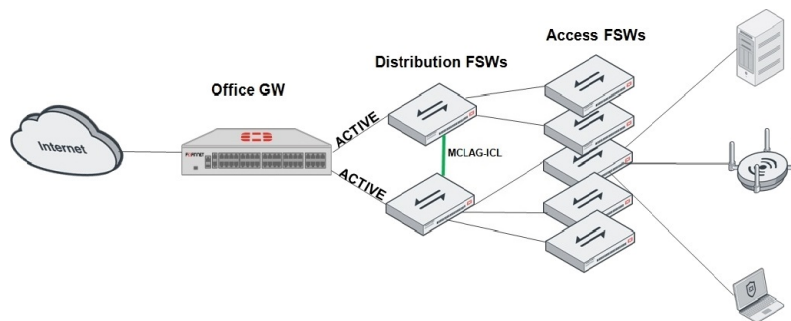
--- 2.2.2.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.1/6.3/13.9 ms
```

## Multiple FortiSwitches in tiers via aggregate interface with MCLAG enabled only on distribution

This example provides a recommended configuration of FortiLink where multi-tier FortiSwitches are managed by a standalone FortiGate as switch controller via aggregate interface, where the FortiGate can provide active-active links to two distribution FortiSwitches connected to each other by MCLAG.

### Prerequisites:

- The FortiGate model supports an aggregate interface.
- FortiSwitch units have been upgraded to latest released software version.
- Layer-3 path/route in the management VDOM is available to Internet so that the FortiSwitch units can synchronize NTP.
- For the FortiSwitch D series, the models above 4 just support MCLAG. For the FortiSwitch E series, the models above 2 just support MCLAG.



### Change the FortiSwitch management mode to FortiLink:

Enter the following CLI commands on the FortiSwitch:

```
config system global
 set switch-mgmt-mode fortilink
end
This operation will cleanup all of the configuration and reboot the system!
Do you want to continue? (y/n)y
Backing up local mode config before entering FortiLink mode....
```

If the FortiSwitch ports used for the FortiLink connection have `auto-discovery-fortilink` enabled, executing authorization on FortiGate will trigger the transformation to FortiLink mode automatically.

```
config switch interface
 edit "port1"
 set auto-discovery-fortilink enable

next
end
```

### Create an aggregate interface and designate it as Fortilink interface on the FortiGate:

Using the CLI:

```
config system interface
 edit "aggr1"
 set vdom "vdom1"
 set fortilink enable
 set type aggregate
 set member "port11" "port12"
 set fortilink-split-interface disable
 next
end
```

`fortilink-split-interface` must be disabled for MCLAG to work.

Using the GUI:

1. Go to *WiFi & Switch Controller > FortiLink Interface*.
2. In *Interface members*, select one or more physical ports that are connected to different distribution FortiSwitches to create an aggregate interface.
3. Disable *FortiLink split interface*.
4. Configure other fields as necessary.
5. Click *OK*.

## Discover and authorize the FortiSwitch:

Using the CLI:

```
config switch-controller managed-switch
 edit "FSWSerialNum"
 set fsw-wan1-admin enable

 next
end
```

Check the CLI output for Connection: Connected to show that FortiLink is up:

```
execute switch-controller get-conn-status FSWSerialNum
```

```
Get managed-switch S248EPTF18001384 connection status:
Admin Status: Authorized
Connection: Connected
Image Version: S248EP-v6.2.0-build143,190107 (Interim)
Remote Address: 2.2.2.2
Join Time: Fri Jan 11 15:22:32 2019
```

interface	status	duplex	speed	fortilink	stacking	poe status
port1	up	full	1000Mbps	no	no	Delivering Power
port2	down	N/A	0	no	no	Searching
.....						

Using the GUI:

1. Go to *WiFi & Switch Controller > Managed FortiSwitch*.
2. Click *Authorize* and wait for a few minutes for the connection to be established.  
When FortiLink between the FortiGate and FortiSwitch is established, the Link-up ports change to green and the POE port that is supplying power changes to blue. The dotted line between the FortiGate and FortiSwitch changes to a solid line. The Connection status shows that FortiLink is up.

## Enable MCLAG on the ICL link between the distribution FortiSwitch devices:

```
conf switch trunk
 edit "4DN4K15000008-0"
 set mclag-icl enable
 next
end
```

When you enable `mclag-icl`, MCLAG on the FortiLink interface is enabled automatically and active-active backup links between the distribution FortiSwitches are established.

## Extend the security perimeter to the edge of FortiSwitch:

1. Configure the VLAN arrangement.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch VLANs*.
  - b. Configure the VLAN interfaces that are applied on FortiSwitch.  
On FortiGate, these switch VLAN interfaces are treated as layer-3 interfaces and are available to be applied by firewall policy and other security controls in FortiOS. This means that security boundary is extended to FortiSwitch.

2. Configure FortiSwitch ports.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch Ports*.
  - b. Select one or more FortiSwitch ports and assign them to the switch VLAN.
  - c. You can also select *POE/DHCP Snooping*, *STP*, and other parameters for the FortiSwitch ports to show their real-time status such as link status, data statistics, etc.
3. Configure access authentication.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch Security Policies*.
  - b. Configure the *802.1X* security policies.
  - c. Select *Port-based* or *MAC-based* mode and select *User groups* from the existing VDOM.
  - d. Configure other fields as necessary.
  - e. Go to *WiFi & Switch Controller > FortiSwitch Ports*.
  - f. Select one or more FortiSwitch ports, click + in the *Security Policy* column, then make a selection from the pane.

## Troubleshooting

### Authorized FortiSwitch always offline

If an authorized FortiSwitch is always offline, go to the FortiGate CLI and use the command below to see all the checkpoints. Inspect each checkpoint to find the cause of the problem.

```
execute switch-controller diagnose-connection S248EPTF18001384

Fortilink interface ... OK
aggr1 enabled

DHCP server ... OK
aggr1 enabled

NTP server ... OK
aggr1 enabled
NTP server sync ... OK
synchronized: yes, ntpsync: enabled, server-mode: enabled

ipv4 server(ntp1.fortiguard.com) 208.91.113.70 -- reachable(0x80) S:2 T:128
no data
ipv4 server(ntp2.fortiguard.com) 208.91.113.71 -- reachable(0x80) S:2 T:128
no data
ipv4 server(ntp2.fortiguard.com) 208.91.112.51 -- reachable(0xff) S:2 T:66 selected
server-version=4, stratum=2
reference time is dfe3aec5.744404e6 -- UTC Sat Jan 12 00:09:41 2019
clock offset is -0.320411 sec, root delay is 0.054535 sec
root dispersion is 0.533081 sec, peer dispersion is 11495 msec

ipv4 server(ntp1.fortiguard.com) 208.91.112.50 -- reachable(0xff) S:2 T:66
server-version=4, stratum=2
reference time is dfe3aec5.744404e6 -- UTC Sat Jan 12 00:09:41 2019
clock offset is -0.448087 sec, root delay is 0.054535 sec
root dispersion is 0.533081 sec, peer dispersion is 12542 msec

HA mode ... disabled

Fortilink
```

```
Status ... SWITCH_AUTHORIZED_READY
Last keepalive ... 1 seconds ago

CAPWAP
Remote Address: 2.2.2.2
Status ... CONNECTED
Last keepalive ... 26 seconds ago

PING 2.2.2.2 (2.2.2.2): 56 data bytes
64 bytes from 2.2.2.2: icmp_seq=0 ttl=64 time=1.1 ms
64 bytes from 2.2.2.2: icmp_seq=1 ttl=64 time=13.9 ms
64 bytes from 2.2.2.2: icmp_seq=2 ttl=64 time=12.7 ms
64 bytes from 2.2.2.2: icmp_seq=3 ttl=64 time=2.9 ms
64 bytes from 2.2.2.2: icmp_seq=4 ttl=64 time=1.2 ms

--- 2.2.2.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.1/6.3/13.9 ms
```

## HA (A-P) mode FortiGate pairs as switch controller

The following recipes provide instructions on configuring a FortiGate HA in Active-Passive (A-P) mode as a switch controller:

- [Multiple FortiSwitches managed via hardware/software switch on page 1586](#)
- [Multiple FortiSwitches in tiers via aggregate interface with redundant link enabled on page 1590](#)
- [Multiple FortiSwitches in tiers via aggregate interface with MCLAG enabled on all tiers on page 1594](#)

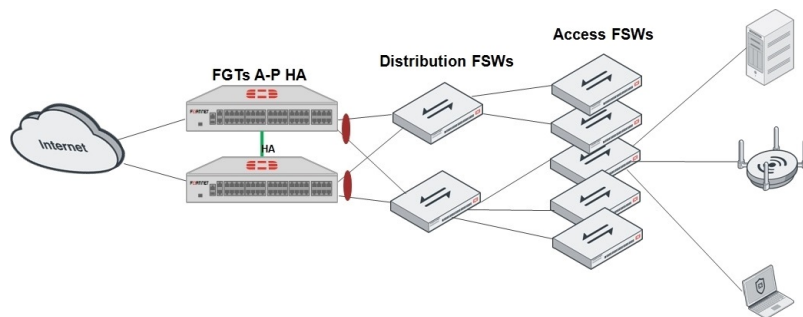
## Multiple FortiSwitches managed via hardware/software switch

This example provides a recommended configuration of FortiLink where multiple FortiSwitches are managed by an A-P mode HA cluster of FortiGates as switch controller via hardware or software switch interface. An example of common usage is when you need multiple distribution FortiSwitches but lack supporting aggregate on the FortiGate pairs.

### Prerequisites:

- The FortiGate model supports hardware or software switch interface.
- FortiSwitch units have been upgraded to latest released software version.
- Layer-3 path/route in the management VDOM is available to Internet so that the FortiSwitch units can synchronize NTP.





### Change the FortiSwitch management mode to FortiLink:

Enter the following CLI commands on the FortiSwitch:

```
config system global
 set switch-mgmt-mode fortilink
end
This operation will cleanup all of the configuration and reboot the system!
Do you want to continue? (y/n)y
Backing up local mode config before entering FortiLink mode....
```

If the FortiSwitch ports used for the FortiLink connection have `auto-discovery-fortilink` enabled, executing authorization on FortiGate will trigger the transformation to FortiLink mode automatically.

```
config switch interface
 edit "port1"
 set auto-discovery-fortilink enable

 next
end
```

### Set up an A-P mode HA cluster:

See [HA active-passive cluster setup on page 698](#).

### Create hardware or software switch interface and designate it as FortiLink interface on the FortiGate:

Create a hardware switch using the CLI:

```
config system virtual-switch
 edit "hardswitch1"
 set physical-switch "sw0"
 config port
 edit "port11"
 next
 edit "port12"
 next
 end
next
end
```

Create a software switch using the CLI:

```
config system switch-interface
 edit "softswitch1"
```

```

 set vdom "vdom1"
 set member "port11" "port12"
 next
end

```

Using the GUI:

1. Go to *WiFi & Switch Controller > FortiLink Interface*.
2. In *Interface members*, select an existing hardware/software switch interface (if there is one) or select one or more physical ports to create a hardware/software switch interface.
3. Configure other fields as necessary.
4. Click *OK*.

### Discover and authorize the FortiSwitch:

Using the CLI:

```

config switch-controller managed-switch
 edit "FSWSerialNum"
 set fsw-wan1-admin enable

next
end

```

Check the CLI output for *Connection: Connected* to show that FortiLink is up:

```
execute switch-controller get-conn-status FSWSerialNum
```

```

Get managed-switch S248EPTF18001384 connection status:
Admin Status: Authorized
Connection: Connected
Image Version: S248EP-v6.2.0-build143,190107 (Interim)
Remote Address: 2.2.2.2
Join Time: Fri Jan 11 15:22:32 2019

```

interface	status	duplex	speed	fortilink	stacking	poe status
port1	up	full	1000Mbps	no	no	Delivering Power
port2	down	N/A	0	no	no	Searching
.....						

Using the GUI:

1. Go to *WiFi & Switch Controller > Managed FortiSwitch*.
2. Click *Authorize* and wait for a few minutes for the connection to be established.  
When FortiLink between the FortiGate and FortiSwitch is established, the Link-up ports change to green and the POE port that is supplying power changes to blue. The dotted line between the FortiGate and FortiSwitch changes to a solid line. The Connection status shows that FortiLink is up.

### Extend the security perimeter to the edge of FortiSwitch:

1. Configure the VLAN arrangement.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch VLANs*.
  - b. Configure the VLAN interfaces that are applied on FortiSwitch.  
On FortiGate, these switch VLAN interfaces are treated as layer-3 interfaces and are available to be applied by firewall policy and other security controls in FortiOS. This means that security boundary is extended to FortiSwitch.

2. Configure FortiSwitch ports.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch Ports*.
  - b. Select one or more FortiSwitch ports and assign them to the switch VLAN.
  - c. You can also select *POE/DHCP Snooping*, *STP*, and other parameters for the FortiSwitch ports to show their real-time status such as link status, data statistics, etc.
3. Configure access authentication.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch Security Policies*.
  - b. Configure the *802.1X* security policies.
  - c. Select *Port-based* or *MAC-based* mode and select *User groups* from the existing VDOM.
  - d. Configure other fields as necessary.
  - e. Go to *WiFi & Switch Controller > FortiSwitch Ports*.
  - f. Select one or more FortiSwitch ports, click + in the *Security Policy* column, then make a selection from the pane.

## Troubleshooting

### Bind FortiLink on hardware switch interface

Fortinet recommends binding FortiLink on the hardware switch interface. Since the hardware switch interface can leverage hardware chips to forward traffic, it does not consume CPU capacity, unlike a software switch.

### Authorized FortiSwitch always offline

If an authorized FortiSwitch is always offline, go to the FortiGate CLI and use the command below to see all the checkpoints. Inspect each checkpoint to find the cause of the problem.

```
execute switch-controller diagnose-connection S248EPTF18001384
```

```
Fortilink interface ... OK
hardswitch1 enabled
```

```
DHCP server ... OK
hardswitch1 enabled
```

```
NTP server ... OK
hardswitch1 enabled
NTP server sync ... OK
synchronized: yes, ntpsync: enabled, server-mode: enabled
```

```
ipv4 server(ntp1.fortiguard.com) 208.91.113.70 -- reachable(0x80) S:2 T:128
 no data
ipv4 server(ntp2.fortiguard.com) 208.91.113.71 -- reachable(0x80) S:2 T:128
 no data
ipv4 server(ntp2.fortiguard.com) 208.91.112.51 -- reachable(0xff) S:2 T:66 selected
 server-version=4, stratum=2
 reference time is dfe3aec5.744404e6 -- UTC Sat Jan 12 00:09:41 2019
 clock offset is -0.320411 sec, root delay is 0.054535 sec
 root dispersion is 0.533081 sec, peer dispersion is 11495 msec

ipv4 server(ntp1.fortiguard.com) 208.91.112.50 -- reachable(0xff) S:2 T:66
 server-version=4, stratum=2
```

```
reference time is dfe3aec5.744404e6 -- UTC Sat Jan 12 00:09:41 2019
clock offset is -0.448087 sec, root delay is 0.054535 sec
root dispersion is 0.533081 sec, peer dispersion is 12542 msec
```

```
HA mode ... disabled
```

```
Fortilink
```

```
Status ... SWITCH_AUTHORIZED_READY
```

```
Last keepalive ... 1 seconds ago
```

```
CAPWAP
```

```
Remote Address: 2.2.2.2
```

```
Status ... CONNECTED
```

```
Last keepalive ... 26 seconds ago
```

```
PING 2.2.2.2 (2.2.2.2): 56 data bytes
```

```
64 bytes from 2.2.2.2: icmp_seq=0 ttl=64 time=1.1 ms
```

```
64 bytes from 2.2.2.2: icmp_seq=1 ttl=64 time=13.9 ms
```

```
64 bytes from 2.2.2.2: icmp_seq=2 ttl=64 time=12.7 ms
```

```
64 bytes from 2.2.2.2: icmp_seq=3 ttl=64 time=2.9 ms
```

```
64 bytes from 2.2.2.2: icmp_seq=4 ttl=64 time=1.2 ms
```

```
--- 2.2.2.2 ping statistics ---
```

```
5 packets transmitted, 5 packets received, 0% packet loss
```

```
round-trip min/avg/max = 1.1/6.3/13.9 ms
```

### HA sync fails

If HA sync fails, use the command below to diagnose and locate the cause.

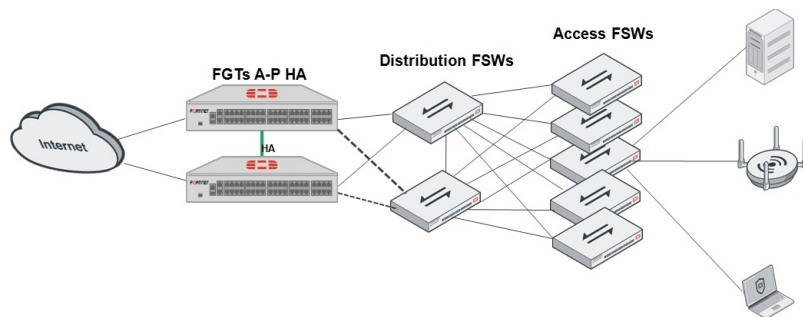
```
diagnose sys ha checksum cluster
```

## Multiple FortiSwitches in tiers via aggregate interface with redundant link enabled

This example provides a recommended configuration of FortiLink where multi-tier FortiSwitches are managed by an A-P mode HA cluster of FortiGates as switch controller via aggregate interface, where each FortiGate cluster member can provide redundant links to multiple ( $\geq 2$ ) distribution FortiSwitches.

### Prerequisites:

- The FortiGate model supports an aggregate interface.
- FortiSwitch units have been upgraded to latest released software version.
- Layer-3 path/route in the management VDOM is available to Internet so that the FortiSwitch units can synchronize NTP.



## Change the FortiSwitch management mode to FortiLink:

Enter the following CLI commands on the FortiSwitch:

```
config system global
 set switch-mgmt-mode fortilink
end
This operation will cleanup all of the configuration and reboot the system!
Do you want to continue? (y/n)y
Backing up local mode config before entering FortiLink mode....
```

If the FortiSwitch ports used for the FortiLink connection have `auto-discovery-fortilink` enabled, executing authorization on FortiGate will trigger the transformation to FortiLink mode automatically.

```
config switch interface
 edit "port1"
 set auto-discovery-fortilink enable

 next
end
```

## Set up an A-P mode HA cluster:

See [HA active-passive cluster setup on page 698](#).

## Create an aggregate interface and designate it as Fortilink interface on the FortiGate:

Using the CLI:

```
config system interface
 edit "aggr1"
 set vdom "vdom1"
 set fortilink enable
 set type aggregate
 set member "port11" "port12"
 set fortilink-split-interface enable
 next
end
```

Using the GUI:

1. Go to *WiFi & Switch Controller > FortiLink Interface*.
2. In *Interface members*, select one or more physical ports that are connected to different distribution FortiSwitches to create an aggregate interface.
3. Enable *FortiLink split interface*.

4. Configure other fields as necessary.
5. Click **OK**.

### Discover and authorize the FortiSwitch:

Using the CLI:

```
config switch-controller managed-switch
 edit "FSWSerialNum"
 set fsw-wan1-admin enable

 next
end
```

Check the CLI output for **Connection: Connected** to show that FortiLink is up:

```
execute switch-controller get-conn-status FSWSerialNum
```

```
Get managed-switch S248EPTF18001384 connection status:
```

```
Admin Status: Authorized
```

```
Connection: Connected
```

```
Image Version: S248EP-v6.2.0-build143,190107 (Interim)
```

```
Remote Address: 2.2.2.2
```

```
Join Time: Fri Jan 11 15:22:32 2019
```

interface	status	duplex	speed	fortilink	stacking	poe status
port1	up	full	1000Mbps	no	no	Delivering Power
port2	down	N/A	0	no	no	Searching
.....						

Using the GUI:

1. Go to *WiFi & Switch Controller > Managed FortiSwitch*.
2. Click **Authorize** and wait for a few minutes for the connection to be established.  
When FortiLink between the FortiGate and FortiSwitch is established, the Link-up ports change to green and the POE port that is supplying power changes to blue. The dotted line between the FortiGate and FortiSwitch changes to a solid line. The Connection status shows that FortiLink is up.

### Extend the security perimeter to the edge of FortiSwitch:

1. Configure the VLAN arrangement.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch VLANs*.
  - b. Configure the VLAN interfaces that are applied on FortiSwitch.  
On FortiGate, these switch VLAN interfaces are treated as layer-3 interfaces and are available to be applied by firewall policy and other security controls in FortiOS. This means that security boundary is extended to FortiSwitch.
2. Configure FortiSwitch ports.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch Ports*.
  - b. Select one or more FortiSwitch ports and assign them to the switch VLAN.
  - c. You can also select *POE/DHCP Snooping*, *STP*, and other parameters for the FortiSwitch ports to show their real-time status such as link status, data statistics, etc.
3. Configure access authentication.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch Security Policies*.
  - b. Configure the *802.1X* security policies.

- c. Select *Port-based* or *MAC-based* mode and select *User groups* from the existing VDOM.
- d. Configure other fields as necessary.
- e. Go to *WiFi & Switch Controller > FortiSwitch Ports*.
- f. Select one or more FortiSwitch ports, click + in the *Security Policy* column, then make a selection from the pane.

## Troubleshooting

### Authorized FortiSwitch always offline

If an authorized FortiSwitch is always offline, go to the FortiGate CLI and use the command below to see all the checkpoints. Inspect each checkpoint to find the cause of the problem.

```
execute switch-controller diagnose-connection S248EPTF18001384
```

```
Fortilink interface ... OK
aggr1 enabled
```

```
DHCP server ... OK
aggr1 enabled
```

```
NTP server ... OK
aggr1 enabled
NTP server sync ... OK
synchronized: yes, ntpsync: enabled, server-mode: enabled
```

```
ipv4 server(ntp1.fortiguard.com) 208.91.113.70 -- reachable(0x80) S:2 T:128
 no data
ipv4 server(ntp2.fortiguard.com) 208.91.113.71 -- reachable(0x80) S:2 T:128
 no data
ipv4 server(ntp2.fortiguard.com) 208.91.112.51 -- reachable(0xff) S:2 T:66 selected
 server-version=4, stratum=2
 reference time is dfe3aec5.744404e6 -- UTC Sat Jan 12 00:09:41 2019
 clock offset is -0.320411 sec, root delay is 0.054535 sec
 root dispersion is 0.533081 sec, peer dispersion is 11495 msec
```

```
ipv4 server(ntp1.fortiguard.com) 208.91.112.50 -- reachable(0xff) S:2 T:66
 server-version=4, stratum=2
 reference time is dfe3aec5.744404e6 -- UTC Sat Jan 12 00:09:41 2019
 clock offset is -0.448087 sec, root delay is 0.054535 sec
 root dispersion is 0.533081 sec, peer dispersion is 12542 msec
```

```
HA mode ... disabled
```

```
Fortilink
Status ... SWITCH_AUTHORIZED_READY
Last keepalive ... 1 seconds ago
```

```
CAPWAP
Remote Address: 2.2.2.2
Status ... CONNECTED
Last keepalive ... 26 seconds ago
```

```

PING 2.2.2.2 (2.2.2.2): 56 data bytes
64 bytes from 2.2.2.2: icmp_seq=0 ttl=64 time=1.1 ms
64 bytes from 2.2.2.2: icmp_seq=1 ttl=64 time=13.9 ms
64 bytes from 2.2.2.2: icmp_seq=2 ttl=64 time=12.7 ms
64 bytes from 2.2.2.2: icmp_seq=3 ttl=64 time=2.9 ms
64 bytes from 2.2.2.2: icmp_seq=4 ttl=64 time=1.2 ms

--- 2.2.2.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.1/6.3/13.9 ms

```

## HA sync fails

If HA sync fails, use the command below to diagnose and locate the cause.

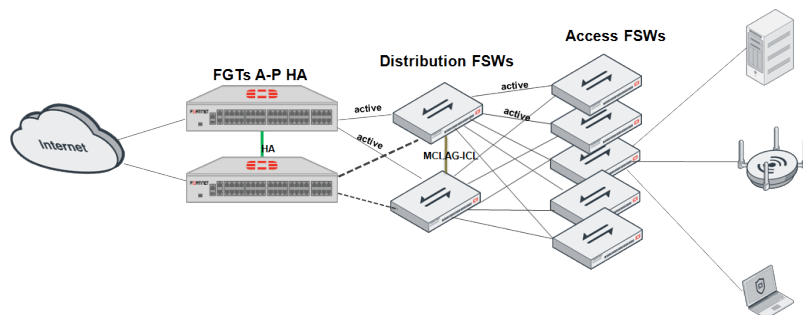
```
diagnose sys ha checksum cluster
```

## Multiple FortiSwitches in tiers via aggregate interface with MCLAG enabled on all tiers

This example provides a recommended configuration of FortiLink where multi-tier FortiSwitch devices are managed by an A-P mode HA cluster of FortiGate devices acting as a switch controller via an aggregate interface. The FortiGates provide A-A links to two distribution FortiSwitches that are connected to each other by MCLAG. All access FortiSwitch devices have A-A links with two upper tier FortiSwitches, as long as the MCLAG-ICL has been enabled between the upper tiers.

### Prerequisites:

- The FortiGate model supports an aggregate interface.
- FortiSwitch units have been upgraded to latest released software version.
- Layer-3 path/route in the management VDOM is available to Internet so that the FortiSwitch units can synchronize NTP.



### Change the FortiSwitch management mode to FortiLink:

Enter the following CLI commands on the FortiSwitch:

```

config system global
 set switch-mgmt-mode fortilink
end
This operation will cleanup all of the configuration and reboot the system!
Do you want to continue? (y/n)y
Backing up local mode config before entering FortiLink mode....

```



If the FortiSwitch ports used for the FortiLink connection have `auto-discovery-fortilink` enabled, executing authorization on FortiGate will trigger the transformation to FortiLink mode automatically.

```
config switch interface
 edit "port1"
 set auto-discovery-fortilink enable

 next
end
```

### Set up an A-P mode HA cluster:

See [HA active-passive cluster setup on page 698](#).

### Create an aggregate interface and designate it as Fortilink interface on the FortiGate:

Using the CLI:

```
config system interface
 edit "aggr1"
 set vdom "vdom1"
 set fortilink enable
 set type aggregate
 set member "port11" "port12"
 set fortilink-split-interface disable
 next
end
```

`fortilink-split-interface` must be disabled for MCLAG to work.

Using the GUI:

1. Go to *WiFi & Switch Controller > FortiLink Interface*.
2. In *Interface members*, select one or more physical ports that are connected to different distribution FortiSwitches to create an aggregate interface.
3. Disable *FortiLink split interface*.
4. Configure other fields as necessary.
5. Click *OK*.

### Discover and authorize the FortiSwitch:

Using the CLI:

```
config switch-controller managed-switch
 edit "FSWSerialNum"
 set fsw-wan1-admin enable

 next
end
```

Check the CLI output for `Connection: Connected` to show that FortiLink is up:

```
execute switch-controller get-conn-status FSWSerialNum

Get managed-switch S248EPTF18001384 connection status:
Admin Status: Authorized
Connection: Connected
```

```
Image Version: S248EP-v6.2.0-build143,190107 (Interim)
Remote Address: 2.2.2.2
Join Time: Fri Jan 11 15:22:32 2019
```

interface	status	duplex	speed	fortilink	stacking	poe status
port1	up	full	1000Mbps	no	no	Delivering Power
port2	down	N/A	0	no	no	Searching
.....						

Using the GUI:

1. Go to *WiFi & Switch Controller > Managed FortiSwitch*.
2. Click *Authorize* and wait for a few minutes for the connection to be established.  
When FortiLink between the FortiGate and FortiSwitch is established, the Link-up ports change to green and the POE port that is supplying power changes to blue. The dotted line between the FortiGate and FortiSwitch changes to a solid line. The Connection status shows that FortiLink is up.

### Enable MCLAG on the ICL link between the distribution FortiSwitch devices:

```
conf switch trunk
edit "4DN4K15000008-0"
set mclag-icl enable
next
end
```

When you enable `mclag-icl`, MCLAG on the FortiLink interface is enabled automatically and active-active backup links between the distribution FortiSwitches are established.

### Extend the security perimeter to the edge of FortiSwitch:

1. Configure the VLAN arrangement.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch VLANs*.
  - b. Configure the VLAN interfaces that are applied on FortiSwitch.  
On FortiGate, these switch VLAN interfaces are treated as layer-3 interfaces and are available to be applied by firewall policy and other security controls in FortiOS. This means that security boundary is extended to FortiSwitch.
2. Configure FortiSwitch ports.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch Ports*.
  - b. Select one or more FortiSwitch ports and assign them to the switch VLAN.
  - c. You can also select *POE/DHCP Snooping*, *STP*, and other parameters for the FortiSwitch ports to show their real-time status such as link status, data statistics, etc.
3. Configure access authentication.
  - a. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch Security Policies*.
  - b. Configure the *802.1X* security policies.
  - c. Select *Port-based* or *MAC-based* mode and select *User groups* from the existing VDOM.
  - d. Configure other fields as necessary.
  - e. Go to *WiFi & Switch Controller > FortiSwitch Ports*.
  - f. Select one or more FortiSwitch ports, click + in the *Security Policy* column, then make a selection from the pane.

## Troubleshooting

### Authorized FortiSwitch always offline

If an authorized FortiSwitch is always offline, go to the FortiGate CLI and use the command below to see all the checkpoints. Inspect each checkpoint to find the cause of the problem.

```
execute switch-controller diagnose-connection S248EPTF18001384

Fortilink interface ... OK
aggr1 enabled

DHCP server ... OK
aggr1 enabled

NTP server ... OK
aggr1 enabled
NTP server sync ... OK
synchronized: yes, ntpsync: enabled, server-mode: enabled

ipv4 server(ntp1.fortiguard.com) 208.91.113.70 -- reachable(0x80) S:2 T:128
no data
ipv4 server(ntp2.fortiguard.com) 208.91.113.71 -- reachable(0x80) S:2 T:128
no data
ipv4 server(ntp2.fortiguard.com) 208.91.112.51 -- reachable(0xff) S:2 T:66 selected
server-version=4, stratum=2
reference time is dfe3aec5.744404e6 -- UTC Sat Jan 12 00:09:41 2019
clock offset is -0.320411 sec, root delay is 0.054535 sec
root dispersion is 0.533081 sec, peer dispersion is 11495 msec

ipv4 server(ntp1.fortiguard.com) 208.91.112.50 -- reachable(0xff) S:2 T:66
server-version=4, stratum=2
reference time is dfe3aec5.744404e6 -- UTC Sat Jan 12 00:09:41 2019
clock offset is -0.448087 sec, root delay is 0.054535 sec
root dispersion is 0.533081 sec, peer dispersion is 12542 msec

HA mode ... disabled

Fortilink
Status ... SWITCH_AUTHORIZED_READY
Last keepalive ... 1 seconds ago

CAPWAP
Remote Address: 2.2.2.2
Status ... CONNECTED
Last keepalive ... 26 seconds ago

PING 2.2.2.2 (2.2.2.2): 56 data bytes
64 bytes from 2.2.2.2: icmp_seq=0 ttl=64 time=1.1 ms
64 bytes from 2.2.2.2: icmp_seq=1 ttl=64 time=13.9 ms
64 bytes from 2.2.2.2: icmp_seq=2 ttl=64 time=12.7 ms
64 bytes from 2.2.2.2: icmp_seq=3 ttl=64 time=2.9 ms
64 bytes from 2.2.2.2: icmp_seq=4 ttl=64 time=1.2 ms
```

```
--- 2.2.2.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.1/6.3/13.9 ms
```

## HA sync fails

If HA sync fails, use the command below to diagnose and locate the cause.

```
diagnose sys ha checksum cluster
```

## Authentication and security

The following recipes provide instructions on configuring switch related authentication and security:

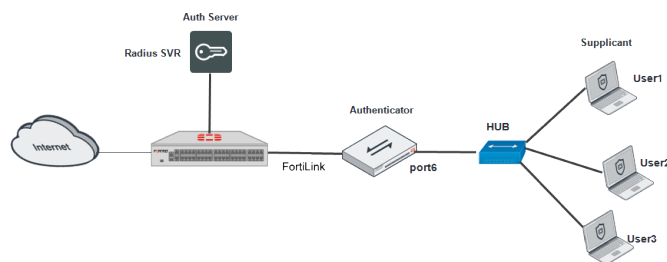
- [MAC-based 802.1X authentication on page 1598](#)
- [Port-based 802.1X authentication on page 1601](#)
- [MAC layer control - Sticky MAC and MAC Learning-limit on page 1604](#)
- [Quarantine on page 1606](#)

## MAC-based 802.1X authentication

This example show how to configure MAC-based 802.1X authentication to managed FortiSwitch ports when using FortiLink. Managed FortiSwitch devices will authenticate and record the MAC addresses of user devices. If there is a hub after the FortiSwitch that connects multiple user devices, each device can access the network after passing authentication.

### Prerequisites:

- The certificates and authentication protocol supported by the supplicant software and RADIUS server are compatible.
- The managed FortiSwitches using FortiLink act as authenticators.



**Create a firewall policy to allow the RADIUS authentication related traffic from the Fortilink interface to the outbound interface on the FortiGate:**

```
config firewall policy
 edit 0
 set srcintf "fortilink-interface"
 set dstintf "outbound-interface-to-RadiusSVR"
 set srcaddr "all"
```

```

 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "RADIUS"
 set nat enable
 next
end

```

## Designate a RADIUS server and create a user group:

Using the CLI:

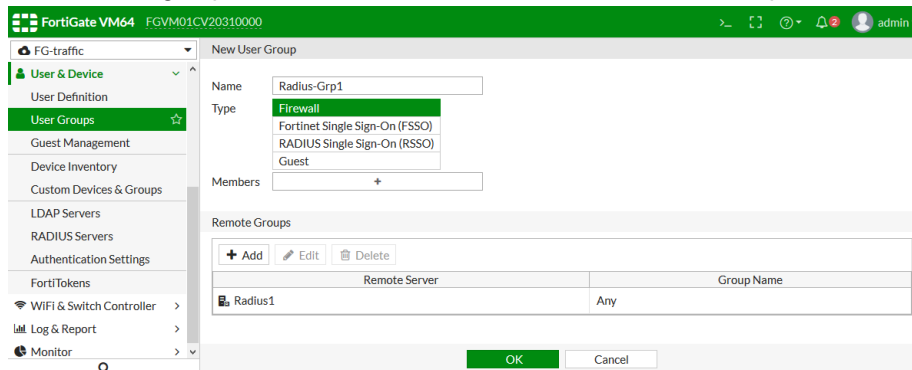
```

config user radius
 edit "Radius1"
 set server "172.18.60.203"
 set secret ENC 1ddddd
 next
end
config user group
 edit "Radius-Grp1"
 set member "Radius1"
 next
end

```

Using the GUI:

1. On the FortiGate, go to *User & Device > RADIUS Servers*.
2. Edit an existing server, or create a new one.
3. If necessary, add a *Name* for the server.
4. Set the *IP/Name* to *172.18.60.203* and *Secret* to *1ddddd*.
5. Configure other fields as necessary.
6. Click *OK*.
7. Go to *User & Device > User Groups*.
8. Create a new group, and add the RADIUS server to the *Remote Groups* list.



9. Click *OK*.

## Use the new user group in a security policy:

Using the CLI:

```

config switch-controller security-policy 802-1X
 edit "802-1X-policy-default"

```

```

 set security-mode 802.1X-mac-based
 set user-group "Radius-Grp1"
 set mac-auth-bypass disable
 set open-auth disable
 set eap-passthru enable
 set guest-vlan disable
 set auth-fail-vlan disable
 set framevid-apply enable
 set radius-timeout-overwrite disable
 next
end

```

Configure the guest VLAN, authentication fail VLAN, and other parameters as needed.

Using the GUI:

1. Go to *WiFi & Switch Controller > FortiSwitch Security Policies*
2. Use the default *802-1X-policy-default*, or create a new security policy.
3. Use the RADIUS server group in the policy.
4. Set the *Security mode* to *MAC-based*.
5. Configure other fields as necessary.
6. Click *OK*.

### Apply the security policy to the ports of the managed FortiSwitches:

Using the CLI:

```

config switch-controller managed-switch
 edit S248EPTF1800XXXX
 config ports
 edit "port6"
 set port-security-policy "802-1X-policy-default"
 next
 end
 next
end

```

On the FortiSwitch, check the configuration:

```

config switch interface
 edit "port6"
 set allowed-vlans 4093
 set untagged-vlans 4093
 set security-groups "Radius-Grp1"
 set snmp-index 6
 config port-security
 set auth-fail-vlan disable
 set eap-passthru enable
 set framevid-apply enable
 set guest-auth-delay 30
 set guest-vlan disable
 set mac-auth-bypass disable
 set open-auth disable
 set port-security-mode 802.1X-mac-based
 set radius-timeout-overwrite disable
 set auth-fail-vlanid 200
 set guest-vlanid 100
 end
 end
end

```

```

 end
 next
end

```

Using the GUI:

1. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch VLANs*.
2. Configure the VLAN interfaces that are applied on FortiSwitch.

On FortiGate, these switch VLAN interfaces are treated as layer-3 interfaces and are available to be applied by firewall policy and other security controls in FortiOS. This means that security boundary is extended to FortiSwitch.

### Execute 802.1X authentication on a user device:

On Linux, run wpa\_supplicant:

```
wpa_supplicant -c /etc/wpa_supplicant/local_supplicant.conf -D wired -i eth2 -dd
```

On the FortiGate, view the status of the 802.1X authentication:

```

diagnose switch-controller switch-info 802.1X
Managed Switch : S248EPTF1800XXXX

port6 : Mode: mac-based (mac-by-pass disable) -----> MAC-based
Link: Link up
Port State: authorized: () -----> Showing authorized means
auth passed. Otherwise, shown failed
EAP pass-through mode : Enable
Native Vlan : 1
Allowed Vlan list: 1,4093
Untagged Vlan list: 1,4093
Guest VLAN :
Auth-Fail Vlan :

Switch sessions 1/240, Local port sessions:1/20
Client MAC Type Vlan Dynamic-Vlan
00:0c:29:d4:4f:3c 802.1x 1 0 -----> User device of
auth passed can access the network. Its MAC address is recored, while other User Devices
under same FSW ports still not allowed to access.

Sessions info:
00:0c:29:d4:4f:3c Type=802.1x,MD5,state=AUTHENTICATED,etime=6,eap_cnt=3
params:reAuth=3600

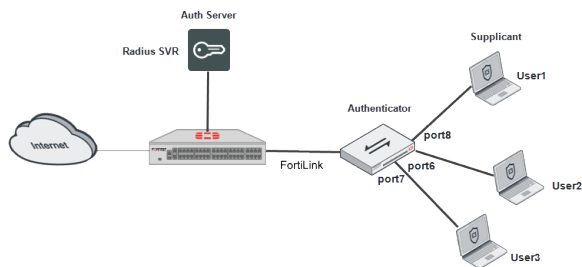
```

## Port-based 802.1X authentication

This example show how to configure Port-based 802.1X authentication to managed FortiSwitch ports when using FortiLink. Managed FortiSwitch devices will authenticate user devices per each FortiSwitch port. If there is a hub after the FortiSwitch that connects multiple user devices to the same port, they can all access the network after authentication, which is not recommended from a security perspective.

### Prerequisites:

- The certificates and authentication protocol supported by the supplicant software and RADIUS server are compatible.
- The managed FortiSwitches using FortiLink act as authenticators.



**Create a firewall policy to allow the RADIUS authentication related traffic from the Fortilink interface to the outbound interface on the FortiGate:**

```

config firewall policy
 edit 0
 set srcintf "fortilink-interface"
 set dstintf "outbound-interface-to-RadiusSVR"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "RADIUS"
 set nat enable
 next
end

```

**Designate a RADIUS server and create a user group:**

Using the CLI:

```

config user radius
 edit "Radius1"
 set server "172.18.60.203"
 set secret ENC 1ddddd
 next
end
config user group
 edit "Radius-Grp1"
 set member "Radius1"
 next
end

```

Using the GUI:

1. On the FortiGate, go to *User & Device > RADIUS Servers*.
2. Edit an existing server, or create a new one.
3. If necessary, add a *Name* for the server.
4. Set the *IP/Name* to *172.18.60.203* and *Secret* to *1ddddd*.
5. Configure other fields as necessary.
6. Click *OK*.
7. Go to *User & Device > User Groups*.



8. Create a new group, and add the RADIUS server to the *Remote Groups* list.

The screenshot shows the FortiGate VM64 GUI with the 'New User Group' configuration page. The left sidebar shows the navigation menu with 'User Groups' selected. The main area has the following fields:

- Name:** Radius-Grp1
- Type:** Firewall (selected from a dropdown menu that also includes Fortinet Single Sign-On (FSSO), RADIUS Single Sign-On (RSSO), and Guest).
- Members:** A field with a '+' icon to add members.
- Remote Groups:** A table with columns 'Remote Server' and 'Group Name'. It contains one entry: 'Radius1' for 'Any'.

At the bottom right, there are 'OK' and 'Cancel' buttons.

9. Click OK.

### Use the new user group in a security policy:

Using the CLI:

```
config switch-controller security-policy 802-1X
 edit "802-1X-policy-default"
 set security-mode 802.1X
 set user-group "Radius-Grp1"
 set mac-auth-bypass disable
 set open-auth disable
 set eap-passthru enable
 set guest-vlan disable
 set auth-fail-vlan disable
 set framevid-apply enable
 set radius-timeout-overwrite disable
 next
end
```

Configure the guest VLAN, authentication fail VLAN, and other parameters as needed.

Using the GUI:

1. Go to *WiFi & Switch Controller > FortiSwitch Security Policies*
2. Use the default *802-1X-policy-default*, or create a new security policy.
3. Use the RADIUS server group in the policy.
4. Set the *Security mode* to *Port-based*.
5. Configure other fields as necessary.
6. Click OK.

### Apply the security policy to the ports of the managed FortiSwitches:

Using the CLI:

```
config switch-controller managed-switch
 edit S248EPTF1800XXXX
 config ports
 edit "port6"
 set port-security-policy "802-1X-policy-default"
 next
 end
 end
```

```
 next
end
```

Using the GUI:

1. On the FortiGate, go to *WiFi & Switch Controller > FortiSwitch VLANs*.
2. Configure the VLAN interfaces that are applied on FortiSwitch.

On FortiGate, these switch VLAN interfaces are treated as layer-3 interfaces and are available to be applied by firewall policy and other security controls in FortiOS. This means that security boundary is extended to FortiSwitch.

### Execute 802.1X authentication on a user device:

On Linux, run wpa\_supplicant:

```
wpa_supplicant -c /etc/wpa_supplicant/local_supplicant.conf -D wired -i eth2 -dd
```

On the FortiGate, view the status of the 802.1X authentication:

```
diagnose switch-controller switch-info 802.1X Managed Switch : S248EPTF18001384

port6 : Mode: port-based (mac-by-pass disable)
Link: Link up
Port State: authorized: ()
Dynamic Authorized Vlan : 0
EAP pass-through mode : Enable
Native Vlan : 1
Allowed Vlan list: 1,4093
Untagged Vlan list: 4093
Guest VLAN :
Auth-Fail Vlan :

Sessions info:
00:0c:29:d4:4f:3c Type=802.1x,MD5,state=AUTHENTICATED,etime=0,eap_cnt=6
params:reAuth=3600
```

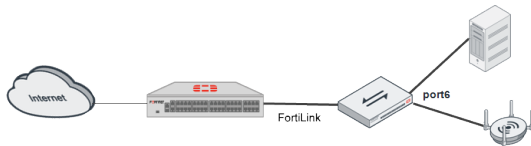
## MAC layer control - Sticky MAC and MAC Learning-limit

Persistent MAC learning, or Sticky MAC, is a port security feature that lets an interface retain dynamically learned MAC addresses when a switch is restarted, or an interface goes down and then is brought back online.

Enabling Sticky MAC along with MAC Learning-limit restricts the number of MAC addresses that are learned. This prevents layer 2 Denial of Service (DoS) attacks, overflow attacks on the Ethernet switching table, and DHCP starvation attacks by limiting the number of MAC addresses that are allowed while still allowing the interface to learn a specified number of MAC addresses. The interface is secured because, after the specified limit has been reached, additional devices cannot connect to the port. Interfaces can be allowed to learn the MAC address of trusted workstations and servers from the time that the interfaces are connected to the network, until the MAC address limit is reached.

### Prerequisites

- Sticky MAC save is hardware and CPU intensive if there are too many entries.
- Dual chip device models (X48 and XX48 FortiSwitch models) do not support MAC Learning-limit on VLANs, but still support it on FortiSwitch ports.



### Enable Sticky MAC on the FortiSwitch ports view:

```
config switch-controller managed-switch
 edit S248EPTF18001384
 config ports
 edit port6
 set sticky-mac enable
 next
 end
 next
end
```

Check the MAC-table on the FortiSwitch to see that the status of related MAC items on the Sticky MAC enabled ports has changed from dynamic to static:

Before Sticky-MAC is enabled:

```
diagnose switch mac-address list
MAC: 08:5b:0e:06:6a:d4 VLAN: 1 Port: port1(port-id 1) Flags: 0x00030440 [hit
dynamic src-hit native move]
```

After Sticky-MAC is enabled:

```
diagnose switch mac-address list
MAC: 00:0c:29:d4:4f:3c VLAN: 1 Port: port6(port-id 6) Flags: 0x00000020 [static]
```

### Save Sticky-MAC items into the database and delete others:

Saving Sticky-MAC items from the running memory into the database, and deleting unsaved items, will ensure that, even after the FortiSwitch is rebooted, the trusted MAC addresses will be kept and will not need to be relearned.

```
execute switch-controller switch-action sticky-mac save all S248EPTF1800XXXX
S248EPTF1800XXXX: Save started...
Warning: Please wait save will take longer time upto 30 seconds...
Collecting config data....Done
Collecting hardware data....Done
Saving....Done
Sticky MAC entries saved = 1 -----> Number of saved Sticky MAC items is
shown

execute switch-controller switch-action sticky-mac delete-unsaved all S248EPTF1800XXXX
```

### Configure the MAC Learning-limit under the VLAN or managed FortiSwitch ports view:

VLAN view:

```
config system interface
 edit vsw.aggr1
 set switch-controller-learning-limit 10
 next
end
```

Ports view:

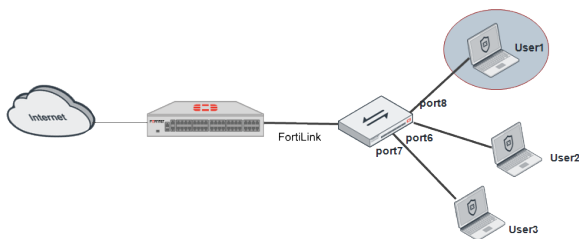
```

config switch-controller managed-switch
 edit S248EPTF1800XXXX
 config ports
 edit port6
 set learning-limit 11
 next
 end
 next
end

```

## Quarantine

When the FortiGate detects devices that have lower trust scores, lack mandatory installed software, or are sending out malicious traffic, an administrator can quarantine the device from the normal switch VLAN to the quarantine VLAN. This can limit the device's access, or provide them specific information on the quarantine portal page.



### To quarantine an active device:

Using the CLI, based on the device's MAC address:

```

config user quarantine
 config targets
 edit "manual-qtn-1"
 set description "Manually quarantined"
 config macs
 edit 00:0c:29:d4:4f:3c
 set description "manual-qtn "
 next
 end
 next
end

```

Using the GUI:

1. On the FortiGate, go to *Security Fabric > Physical Topology*, or *Security Fabric > Logical Topology*.
2. Mouse over the bubble of an active device, and select *Quarantine Host* from the right-click menu.
3. Click *OK* in the *Quarantine Host* page to quarantine the device.

The quarantined device is moved to the quarantine VLAN, and the configuration of the FortiSwitch port does not change.

The quarantined device gets its IP address from the DHCP server on the quarantine VLAN interface. The network locations that the device can access depends on the firewall policies that are configured for the quarantine VLAN interface. By default, the device must acknowledge and accept the information on the Quarantine Portal before it can access any part of the network.

**Release or clear the quarantine targets:**

Using the CLI:

```
config user quarantine
 config targets
 delete "manual-qtn-1"
 ...
 end
end

config user quarantine
 config targets
 purge
 end
end
```

Using the GUI:

1. Go to *Monitor > Quarantine Monitor*.
2. Delete the quarantine targets as needed, or click *Remove All* to delete all the targets.

## Flow and Device Detection

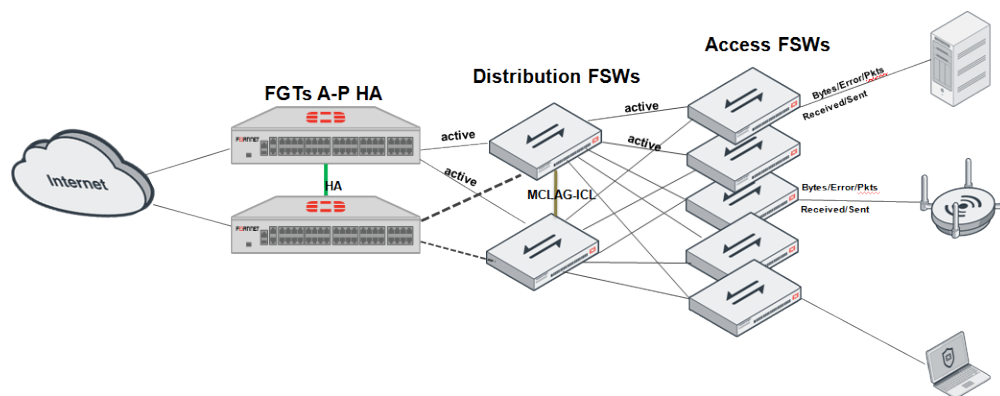
The following recipes provide information on flow and device detection:

- [Data statistic on page 1607](#)
- [Security Fabric showing on page 1608](#)

### Data statistic

This example shows a FortiLink scenario where the FortiGate acts as the switch controller that collects the data statistics of managed FortiSwitch ports. This is counted by each FortiSwitch and concentrated in the controller.

#### Sample topology



### To show data statistics using the GUI:

1. Go to *WiFi & Switch Controller > FortiSwitch Ports*.
2. Select *Configure Table*.
3. Select *Bytes, Errors and Packets* to make them visible.

The related data statistic of each managed FortiSwitch port is shown.

### To show data statistics using the CLI:

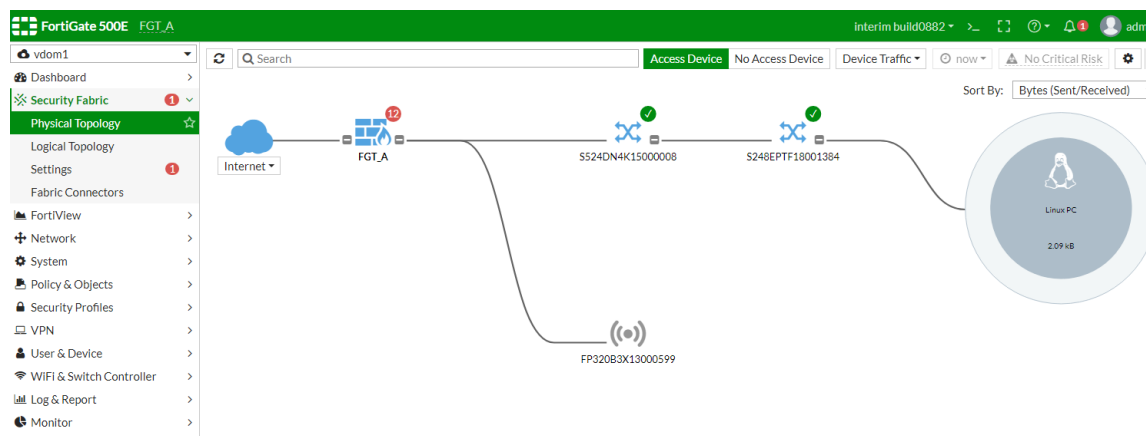
```
diagnose switch-controller switch-info port-stats S248EPTF180XXXX
.....

Port(port50) is Admin up, line protocol is down
Interface Type is Gigabit Media Independent Interface(GMII)
Address is 70:4C:A5:E0:F3:8D, loopback is not set
MTU 9216 bytes, Encapsulation IEEE 802.3/Ethernet-II
full-duplex, 1000 Mb/s, link type is manual
input : 0 bytes, 0 packets, 0 errors, 0 drops, 0 oversizes
 0 unicasts, 0 multicasts, 0 broadcasts, 0 unknowns
output : 0 bytes, 0 packets, 0 errors, 0 drops, 0 oversizes
 0 unicasts, 0 multicasts, 0 broadcasts
 0 fragments, 0 undersizes, 0 collisions, 0 jabbers
.....
```

## Security Fabric showing

This example shows one of the key components in the concept of Security Fabric: FortiSwitches in FortiLink. In the FortiGate GUI, you can see the whole picture of the Security Fabric working for your network security.

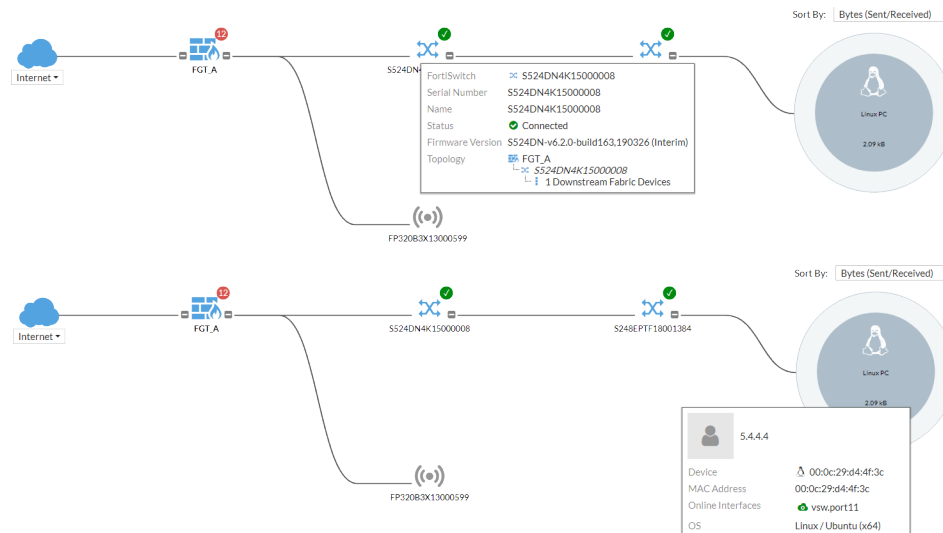
### Sample topology



### To show Security Fabric information:

1. Go to *Security Fabric > Physical Topology*.
2. To see the connection between FortiGates and managed FortiSwitches, hover the pointer over the icons to see

information about each network element.



## FortiSwitch multi-tenant support

A virtual switch provides a container for physical ports to be loaned to other VDOMs, allowing local management of the resource.

The following example shows how to export managed FortiSwitch ports to multitenant VDOMs. In this example, the owner VDOM is `vdom1`, and the tenant VDOM is `root`.

### To export managed FortiSwitch ports to multitenant VDOMs:

1. Configure the switch VLAN interface, and assign it to the tenant VDOM:

```
(vdom1) # config system interface
edit "fsw_vlan"
 set vdom "root"
 set device-identification enable
 set role lan
 set snmp-index 32
 set interface "fsw"
 set vlanid 100
next
end
```

2. In the tenant VDOM, designate the `default-virtual-switch-vlan`, which is used to set the native VLAN of ports leased from the owner VDOM:

```
(root) # config switch-controller global
 set default-virtual-switch-vlan "fsw_vlan"
end
```

3. On `vdom1`, export the managed switch ports to the `root`:

```
(vdom1) # config switch-controller managed-switch
edit S248EPTF1800XXXX
```

```

 set fsw-wan1-peer "fsw"
 set fsw-wan1-admin enable
 set version 1
 set dynamic-capability 100531703
 config ports
 edit "port1"
 set export-to "root"
 next
 ...
 end
 next
end

```

The lease port is now available under the tenant VDOM:

```

(root) # config switch-controller managed-switch
show
 config switch-controller managed-switch
 edit "S248EPTF1800XXXX"
 set type virtual
 set owner-vdom "vdom1"
 config ports
 edit "port1"
 set vlan "fsw_vlan"
 next
 end
 next
 end
end

```

#### 4. Export the managed FortiSwitch port to a virtual port pool for the tenant VDOM to choose from:

```

(vdom1) # config switch-controller virtual-port-pool
 edit "tenant-monthly"
 next
end

(vdom1) # config switch-controller managed-switch
 edit "S248EPTF1800XXXX"
 set fsw-wan1-peer "fsw"
 set fsw-wan1-admin enable
 set version 1
 set dynamic-capability 100531703
 config ports
 edit "port2"
 set vlan "vsw.fsw"
 set allowed-vlans "qtn.fsw"
 set untagged-vlans "qtn.fsw"
 set export-to-pool "tenant-monthly"
 set export-to "vdom1"
 next
 ...
 end
 next
end

```

#### 5. Request the available port in the virtual port pool to use the switch port:

```

(root) # execute switch-controller virtual-port-pool request S248EPTF1800XXXX port2

```



```
(root) # config switch-controller managed-switch
edit "S248EPTF1800XXXX"
set type virtual
set owner-vdom "vdom1"
config ports
edit "port2"
set vlan "fsw_vlan"
next
end
next
end
```

## 6. Return the port after use:

```
(root) # execute switch-controller virtual-port-pool return S248EPTF1800XXXX port2
```

## 7. Configure tags for the switch ports so the tags can be exported to virtual port pools

```
(vdom1) # config switch-controller switch-interface-tag
edit "vip"
next
edit "gold"
next
edit "silver"
next
end

(vdom1) # config switch-controller managed-switch
edit "S248EPTF1800XXXX"
set fsw-wan1-peer "fsw"
set fsw-wan1-admin enable
set version 1
set dynamic-capability 100531703
config ports
edit "port2"
set export-to-pool "tenant-monthly"
set export-tags "silver"
set export-to "root"
next
edit "port3"
set vlan "vsw.fsw"
set allowed-vlans "qtn.fsw"
set untagged-vlans "qtn.fsw"
set export-to-pool "tenant-monthly"
set export-tags "vip"
set export-to "vdom1"
next
edit "port4"
set vlan "vsw.fsw"
set allowed-vlans "qtn.fsw"
set untagged-vlans "qtn.fsw"
set export-to-pool "tenant-monthly"
set export-tags "vip" "silver"
set export-to "vdom1"
next
end
next
end
```

**8. Search for ports using tag filters:**

```
(vdom1) # execute switch-controller virtual-port-pool show-by-tag silver
 Switch Port Properties Tags

tenant-monthly(vdom.vdom1)
 S248EPTF1800XXXX port2 (root) 10M/100M/1G/ silver
 S248EPTF1800XXXX port4 10M/100M/1G/ vip,silver

(vdom1) # exe switch-controller virtual-port-pool show-by-tag vip
 Switch Port Properties Tags

tenant-monthly(vdom.vdom1)
 S248EPTF1800XXXX port3 10M/100M/1G/ vip
 S248EPTF1800XXXX port4 10M/100M/1G/ vip,silver
```

## Persistent MAC learning

Persistent MAC learning or sticky MAC is a port security feature where dynamically learned MAC addresses are retained when a switch or interface comes back online. The benefits of this feature include:

- Prevent traffic loss from trusted workstations and servers since there is no need to relearn MAC address after a restart.
- Protect the switch and the whole network when combined with MAC-learning-limit against security attacks such as Layer 2 DoS and overflow attacks.

Persistent MAC learning is configured in FortiGate and implemented in FortiSwitch.

This feature is disabled by default. You can use persistent MAC learning together with MAC limiting to restrict the number of persistent MAC addresses.

This feature is hardware and CPU intensive and can take several minutes depending on the number of entries.

You can only use CLI to configure this feature.



This feature is supported on all FortiSwitch models in FSW 6.0.

This feature is supported on models in FSW 3.6 higher than the 124D series.

**To enable sticky MAC on FortiGate:**

```
config switch-controller managed-switch
 edit <switch-serial-number>
 conf ports
 edit <port-number>
 set sticky-mac enable
 next
 end
 next
end
```

Before saving sticky Mac entries into CMDB, you might want to delete the unsaved sticky MAC items so that only the items you want are saved.

Saving sticky MAC items copies the sticky MAC items from memory to CMDB on FortiSwitches and FortiGates.

**To delete unsaved sticky MAC items:**

```
execute switch-controller switch-action sticky-mac delete-unsaved <all | interface><switch-serial-number>
```

**To save sticky MAC items into CMDB:**

```
execute switch-controller switch-action sticky-mac save <all | interface><switch-serial-number>
```

## Split port mode (for QSFP / QSFP28)

The quad, small, form-factor pluggable plus (QSFP/QSPF28) is a transceiver module that offers high-density 40/100 Gigabit Ethernet connectivity options for data center and high-performance computing networks. The QSFP transceiver module is a hot-swappable, parallel fiber-optic/copper module with four independent optical transmit and receive channels. These channels can terminate in another Ethernet QSFP transceiver, or the channels can be broken out to four separate physical ports.

Configuration of which FortiSwitch ports are split is controlled directly on the FortiSwitch. An administrator needs to manually log into the FortiSwitch and set the desired split port configuration. After a split port configuration change is made on the FortiSwitch, it will automatically reboot. If the FortiSwitch was previously discovered or authorized, it should be deleted to allow the switch to be newly discovery again.



This feature requires a FortiSwitch model with SFP+ 40G ports, and FortiSwitch must be in Fortlink mode when changing the split configuration.

---

**To use previously discovered FortiSwitch with split ports with the switch controller:**

1. On FortiSwitch, change the split mode:

This change requires a reboot.

```
config switch phy-mode
 set port29-phy-mode 4x10G
 set port30-phy-mode 4x10G
end
```

2. Delete the FortiSwitch from `managed-switch` stanza.
3. Discover and authorize.

**To use FortiSwitch with factory defaults with split ports with the switch controller:**

1. Discover and Authorize.  
This change requires a reboot.
2. On FortiSwitch, change split mode.  
This change requires a reboot.
3. Delete switch from `managed-switch` stanza.
4. Discover and authorize.

```
config switch-controller managed-switch
 edit S524DN4K15000008
 config ports
 edit "port29.1"
 set speed 10000
 set vlan "vsw.port11"
 set allowed-vlans "qtn.port11"
 set untagged-vlans "qtn.port11"
 set export-to "root"
 next

 edit "port29.4"
 set speed 10000
 set vlan "vsw.port11"
 set allowed-vlans "qtn.port11"
 set untagged-vlans "qtn.port11"
 set export-to "root"
 next
 edit "port30.1"
 set speed 10000
 set vlan "vsw.port11"
 set allowed-vlans "qtn.port11"
 set untagged-vlans "qtn.port11"
 set export-to "root"
 next

 edit "port30.4"
 set speed 10000
 set vlan "vsw.port11"
 set allowed-vlans "qtn.port11"
 set untagged-vlans "qtn.port11"
 set export-to "root"
 next
 end
 next
end
```

## Dynamic VLAN name assignment from RADIUS attribute

On the FortiGate, all VLANs are specified as a system interface. Each system interface has a well-defined and unique name. When running FortiLink, the switch has no knowledge of the name association. The switch communicates directly with the RADIUS server and needs to know the mapping to make the proper selection. This information must be provided to the switch.

In order to make the feature generic and applicable to the switch in standalone mode, the system interface description field is leveraged. The switch-controller synchronizes this field to the switch for information purposes. All descriptions on the FortiGate remain on the FortiGate. The switch-controller synchronizes the FortiGate system interface name to the switch VLAN description.

When FortiSwitch receives a VLAN assignment from a RADIUS server, it determines if the data is an integer or string representation. If the representation is an integer, FortiSwitch assigns the VLAN. If the representation is a string, the 802.1x agent searches each FortiGate VLAN description field and, if a match is found, synchronizes the FortiGate

interface name to the switch's VLAN description. If no match is found, it will generate a syslog error stating that the VLAN string was not found, the assignment could not be made, and the result is treated as in unauthorized or a failure.

### To configure dynamic VLAN name assignment:

#### 1. Configure a RADIUS server:

- Set Tunnel-Type to "VLAN"
  - Set Tunnel-Medium-Type to "IEEE-802"
  - Set Tunnel-Private-Group-Id to "my.vlan.10"
- Designate the VLAN name instead of VLAN ID.

#### 2. Configure the FortiGate:

```
config system interface
 edit "my.vlan.10"
 set vdom "root"
 set ip 1.1.1.254 255.255.255.0
 set allowaccess ping
 set interface "my.fortlink"
 set vlanid 10
 next
end
```

#### 3. Configure the FortiSwitch:

```
config switch vlan
 edit 10
 set description "my.vlan.10"
 next
end
```

## MSTI support

Administrators can control multiple spanning tree instances (MSTI) one to 14, and allocate VLANs to specific instances. VLANs that are not added to a specific interface are in MSTI-0. FortiLink controls MSTI-0 (CST) and MSTI-15 for FortiLink management (VLAN 4094).

Each instance is a full and complete spanning tree. Any VLAN can be mapped to any instance, allowing the trees to have different topologies for each MSTI. Various parameters can be configured in each instance, such as cost and priority.

### To configure MSTI support:

#### 1. Create a spanning tree protocol (STP) instance between 1 to 14:

```
config switch-controller stp-instance
 edit 1
 set vlan-range tenant-vlan3 vsw.aggr1
 next
end
```

#### 2. Configure a specific STP priority on different managed FortiSwitch units:

```
config switch-controller managed-switch
 edit S248EPTF1800XXXX
```

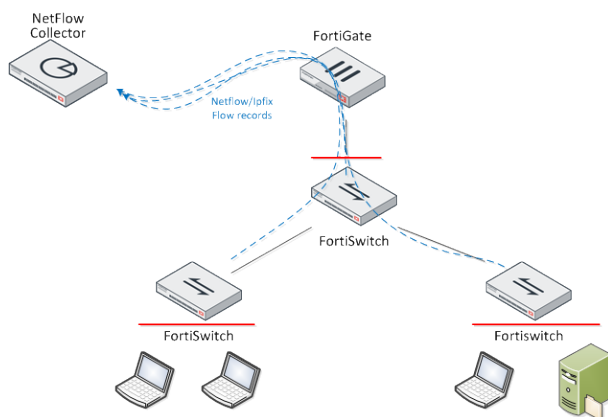
```

config stp-instance
 edit 1
 set priority 8192
 next
end
next
end

```

## Netflow and IPFIX support

You can configure Netflow (v1, v5, and v9) and IP Flow Information Export (IPFIX) on managed FortiSwitch units on switch controller. The resulting data are available in FortiView and to FortiAnalyzer for traffic statistics and topology views. Traffic sampling data can be used to show which users and device behind a switch are generating the most traffic.



The following CLI can be used to configure flow-tracking parameters:

```

config system flow-tracking
 set sample-mode {local | perimeter | device-ingress}
 set sample-rate <integer>
 set format {netflow1 | netflow5 | netflow9 | ipfix}
 set collector-ip <ip_address>
 set collector-port <integer>
 set transport {udp | tcp | sctp}
 set level {vlan | ip | port | proto}
 set max-export-pkt-size <integer>
 set timeout-general <integer>
 set timeout-icmp <integer>
 set timeout-max <integer>
 set timeout-tcp <integer>
 set timeout-tcp-fin <integer>
 set timeout-tcp-rst <integer>
 set timeout-udp <integer>
 config aggregates
 edit <id>
 set ip <ip_address>
 next
 end
end

```

Variable	Description
sample-mode {local   perimeter   device-ingress}	<p>Sample mode for flow tracking.</p> <ul style="list-style-type: none"> <li><b>local:</b> Sample on the specific FortiSwitch port. Sampling must be enabled on the specific FortiSwitch ports using the <code>config switch-controller managed-switch</code> and <code>config ports</code> commands.</li> <li><b>perimeter:</b> Sample on all non-fabric FortiSwitch ports, including the access and FortiLink ports, but not the FortiLink ISL port.</li> <li><b>device-ingress:</b> Sample on all FortiSwitch ports.</li> </ul>
sample-rate <integer>	Sample rate for the perimeter and device-ingress sampling (0 - 99999, default = 512).
format {netflow1   netflow5   netflow9   ipfix}	Flow tracking protocol (default = netflow9).
collector-ip <ip_address>	<p>Collector IP address.</p> <p>An all-zero IP address implies the feature is disabled</p>
collector-port <integer>	Collector port number (0 - 65535, default=0).
transport {udp   tcp   sctp}	L4 transport protocol for exporting packets (default = udp).
level {vlan   ip   port   proto}	<p>Flow tracking level.</p> <ul style="list-style-type: none"> <li><b>vlan:</b> Collect srcip/dstip/srcport/dstport/protocol/tos/vlan from the sample packet.</li> <li><b>ip:</b> Collect srcip/dstip from the sample packet (default).</li> <li><b>port:</b> Collect srcip/dstip/srcport/dstport/protocol from the sample packet.</li> <li><b>proto:</b> Collect srcip/dstip/protocol from the sample packet.</li> </ul>
max-export-pkt-size <integer>	Flow maximum export packet size, in bytes (512 - 9216, default = 512).
timeout-general <integer>	Flow session general timeout, in seconds (60 - 604800, default = 3600).
timeout-icmp <integer>	Flow session ICMP timeout, in seconds (60 - 604800, default = 300).
timeout-max <integer>	Flow session maximum timeout, in seconds (60 - 604800, default = 604800).
timeout-tcp <integer>	Flow session TCP timeout, in seconds (60 - 604800, default = 3600).
timeout-tcp-fin <integer>	Flow session TCP FIN timeout, in seconds (60 - 604800, default = 300).
timeout-tcp-rst <integer>	Flow session TCP RST timeout, in seconds (60 - 604800, default = 120).
timeout-udp <integer>	Flow session UDP timeout, in seconds (60 - 604800, default = 300).
<p><code>config aggregates</code> <b>subcommand:</b></p> <p>Aggregates in which all traffic sessions matching the IP address will be grouped into the same flow.</p>	
ip <ip_address>	IP address to group all matching traffic sessions to a flow.

# Log and Report

Logging and reporting are useful components to help you understand what is happening on your network, and to inform you about certain network activities, such as the detection of a virus, a visit to an invalid website, an intrusion, a failed log in attempt, and myriad others.

Logging records the traffic that passes through, starts from, or ends on the FortiGate, and records the actions the FortiGate took during the traffic scanning process. After this information is recorded in a log message, it is stored in a log file that is stored on a log device (a central storage location for log messages). FortiGates support several log devices, such as FortiAnalyzer, FortiGate Cloud, and syslog servers. Approximately 5% of memory is used for buffering logs sent to FortiAnalyzer. The FortiGate system memory and local disk can also be configured to store logs, so it is also considered a log device.

Reports show the recorded activity in a more readable format. A report gathers all the log information that it needs, then presents it in a graphical format with a customizable design and automatically generated charts showing what is happening on the network. Reports can be generated on FortiGate devices with disk logging and on FortiAnalyzer devices.

FortiView is a more comprehensive network reporting and monitoring tool. It integrates real-time and historical data into a single view in FortiOS. For more information, see [FortiView on page 276](#).



Performance statistics are not logged to disk. Performance statistics can be received by a syslog server or by FortiAnalyzer.

---

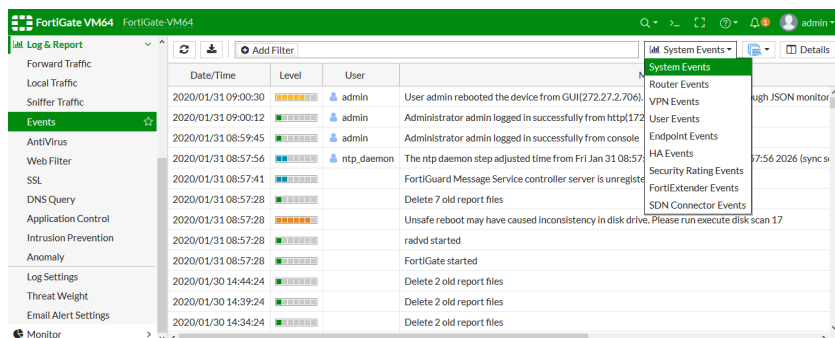
The following topics provide information about logging and reporting:

- [Viewing event logs on page 1618](#)
- [Sample logs by log type on page 1619](#)
- [Checking the email filter log on page 1639](#)
- [Supported log types to FortiAnalyzer, FortiAnalyzer Cloud, FortiGate Cloud, and syslog on page 1640](#)
- [Configuring multiple FortiAnalyzers on a multi-VDOM FortiGate on page 1640](#)
- [Configuring multiple FortiAnalyzers \(or syslog servers\) per VDOM on page 1643](#)
- [Source and destination UUID logging on page 1644](#)
- [Troubleshooting on page 1646](#)

## Viewing event logs

All event log subtypes are available from the event log subtype dropdown list on the *Log & Report > Events* page. Not all of the event log subtypes are available by default.





<b>System Events</b>	Always available.
<b>Router Events</b>	Always available.
<b>VPN Events</b>	Available when <i>VPN</i> is enabled in <i>System &gt; Feature Visibility</i> .
<b>User Events</b>	Always available.
<b>Endpoint Events</b>	Available when <i>Endpoint Control</i> is enabled in <i>System &gt; Feature Visibility</i> .
<b>HA Events</b>	Always available.
<b>Security Rating Events</b>	Always available, but logs are only generated when a Security Rating License is registered.
<b>WAN Opt. &amp; Cache Events</b>	Available on devices with two hard disks by default. On devices with one hard disk, the disk usage must be set to <code>wanopt</code> and then <i>WAN Opt. &amp; Cache</i> must be enabled in <i>System &gt; Feature Visibility</i> .
<b>WiFi Events</b>	Available on hardware devices when <i>WiFi Controller</i> is enabled in <i>System &gt; Feature Visibility</i> .
<b>FortiExtender Events</b>	Available when <i>FortiExtender</i> is enabled in <i>System &gt; Feature Visibility</i> .
<b>SDN Connector Events</b>	Always available.

## Sample logs by log type

This topic provides a sample raw log for each subtype and the configuration requirements.

### Type and Subtype

*Traffic Logs > Forward Traffic*

#### Log configuration requirements

```
config firewall policy
 edit 1
 set srcintf "port12"
 set dstintf "port11"
 set srcaddr "all"
```

```
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set utm-status enable
set logtraffic all
set application-list "g-default"
set ssl-ssh-profile "certificate-inspection"
set nat enable
next
end
```

### Sample log

```
date=2019-05-10 time=11:37:47 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="vdom1" eventtime=1557513467369913239 srcip=10.1.100.11 srcport=58012
srcintf="port12" srcintfrole="undefined" dstip=23.59.154.35 dstport=80 dstintf="port11"
dstintfrole="undefined" srcuuid="ae28f494-5735-51e9-f247-d1d2ce663f4b" dstuuid="ae28f494-
5735-51e9-f247-d1d2ce663f4b" poluuid="ccb269e0-5735-51e9-a218-a397dd08b7eb" sessionid=105048
proto=6 action="close" policyid=1 policytype="policy" service="HTTP" dstcountry="Canada"
srccountry="Reserved" trandisp="snat" transip=172.16.200.2 transport=58012 appid=34050
app="HTTP.BROWSER_Firefox" appcat="Web.Client" apprisk="elevated" applist="g-default"
duration=116 sentbyte=1188 rcvdbyte=1224 sentpkt=17 rcvdpkt=16 utmaction="allow" countapp=1
osname="Ubuntu" mastersrcmac="a2:e9:00:ec:40:01" srcmac="a2:e9:00:ec:40:01" srcserver=0
utmref=65500-742
```

### Type and Subtype

*Traffic Logs > Local Traffic*

#### Log configuration requirements

```
config log setting
set local-in-allow enable
set local-in-deny-unicast enable
set local-in-deny-broadcast enable
set local-out enable
end
```

### Sample log

```
date=2019-05-10 time=11:50:48 logid="0001000014" type="traffic" subtype="local"
level="notice" vd="vdom1" eventtime=1557514248379911176 srcip=172.16.200.254 srcport=62024
srcintf="port11" srcintfrole="undefined" dstip=172.16.200.2 dstport=443 dstintf="vdom1"
dstintfrole="undefined" sessionid=107478 proto=6 action="server-rst" policyid=0
policytype="local-in-policy" service="HTTPS" dstcountry="Reserved" srccountry="Reserved"
trandisp="noop" app="Web Management(HTTPS)" duration=5 sentbyte=1247 rcvdbyte=1719 sentpkt=5
rcvdpkt=6 appcat="unscanned"
```

### Type and Subtype

*Traffic Logs > Multicast Traffic*

## Log configuration requirements

```
config firewall multicast-policy
 edit 1
 set dstaddr 230-1-0-0
 set dstintf port3
 set srcaddr 172-16-200-0
 set srcintf port25
 set action accept
 set log enable
 next
end
config sys setting
 set multicast-forward enable
end
```

## Sample log

```
date=2019-03-31 time=06:42:54 logid="0002000012" type="traffic" subtype="multicast"
level="notice" vd="vdom1" eventtime=1554039772 srcip=172.16.200.55 srcport=60660
srcintf="port25" srcintfrole="undefined" dstip=230.1.1.2 dstport=7878 dstintf="port3"
dstintfrole="undefined" sessionid=1162 proto=17 action="accept" policyid=1
policytype="multicast-policy" service="udp/7878" dstcountry="Reserved" srccountry="Reserved"
trandisp="noop" duration=22 sentbyte=5940 rcvdbyte=0 sentpkt=11 rcvdpkt=0 appcat="unscanned"
```

## Type and Subtype

*Traffic Logs > Sniffer Traffic*

## Log configuration requirements

```
config firewall sniffer
 edit 3
 set logtraffic all
 set interface "port1"
 set ips-sensor-status enable
 set ips-sensor "sniffer-profile"
 next
end
```

## Sample log

```
date=2019-05-10 time=14:18:54 logid="0004000017" type="traffic" subtype="sniffer"
level="notice" vd="root" eventtime=1557523134021045897 srcip=208.91.114.4 srcport=50463
srcintf="port1" srcintfrole="undefined" dstip=104.80.88.154 dstport=443 dstintf="port1"
dstintfrole="undefined" sessionid=2193276 proto=6 action="accept" policyid=3
policytype="sniffer" service="HTTPS" dstcountry="United States" srccountry="Canada"
trandisp="snat" transip=0.0.0.0 transport=0 duration=10 sentbyte=0 rcvdbyte=0 sentpkt=0
rcvdpkt=0 appcat="unscanned" utmaction="allow" countips=1 crscore=5 craction=32768
sentdelta=0 rcvddelta=0 utmref=65162-7772
```

## Type and Subtype

*Event Logs > System Events*

### Log configuration requirements

```
config log eventfilter
 set event enable
 set system enable
end
```

### Sample log

```
date=2019-05-13 time=11:20:54 logid="0100032001" type="event" subtype="system"
level="information" vd="vdom1" eventtime=1557771654587081441 logdesc="Admin login
successful" sn="1557771654" user="admin" ui="ssh(172.16.200.254)" method="ssh"
srcip=172.16.200.254 dstip=172.16.200.2 action="login" status="success" reason="none"
profile="super_admin" msg="Administrator admin logged in successfully from ssh
(172.16.200.254) "
```

### Type and Subtype

*Event Logs > Router Events*

### Log configuration requirements

```
config log eventfilter
 set event enable
 set router enable
end

config router bgp
 set log-neighbour-changes enable
end

config router ospf
 set log-neighbour-changes enable
end
```

### Sample log

```
date=2019-05-13 time=14:12:26 logid="0103020301" type="event" subtype="router"
level="warning" vd="root" eventtime=1557781946677737955 logdesc="Routing log" msg="OSPF:
RECV[Hello]: From 31.1.1.1 via port9:172.16.200.1: Invalid Area ID 0.0.0.0"
```

### Type and Subtype

*Event Logs > VPN Events*

### Log configuration requirements

```
config log eventfilter
 set event enable
 set vpn enable
end
```

## Sample log

```
date=2019-05-13 time=14:21:42 logid="0101037127" type="event" subtype="vpn" level="notice"
vd="root" eventtime=1557782502722231889 logdesc="Progress IPsec phase 1" msg="progress IPsec
phase 1" action="negotiate" remip=50.1.1.101 locip=50.1.1.100 remport=500 locport=500
outintf="port14" cookies="9091f4d4837ea71c/0000000000000000" user="N/A" group="N/A"
xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="test" status="success" init="local"
mode="main" dir="outbound" stage=1 role="initiator" result="OK"
```

## Type and Subtype

*Event Logs > User Events*

### Log configuration requirements

```
config log eventfilter
 set event enable
 set user enable
end
```

## Sample log

```
date=2019-05-13 time=15:55:56 logid="0102043008" type="event" subtype="user" level="notice"
vd="root" eventtime=1557788156913809277 logdesc="Authentication success" srcip=10.1.100.11
dstip=172.16.200.55 policyid=1 interface="port10" user="bob" group="local-group1"
authproto="TELNET(10.1.100.11)" action="authentication" status="success" reason="N/A"
msg="User bob succeeded in authentication"
```

## Type and Subtype

*Event Logs > Endpoint Events*

### Log configuration requirements

```
config log eventfilter
 set event enable
 set endpoint enable
end
```

## Sample log

```
date=2019-05-14 time=08:32:13 logid="0107045057" type="event" subtype="endpoint"
level="information" vd="root" eventtime=1557847933900764210 logdesc="FortiClient connection
added" action="add" status="success" license_limit="unlimited" used_for_type=4 connection_
type="sslvpn" count=1 user="skubas" ip=172.18.64.250 name="VAN-200957-PC"
fctuid="52C66FE08F724FE0B116DAD5062C96CD" msg="Add a FortiClient Connection."

date=2019-05-14 time=08:19:38 logid="0107045058" type="event" subtype="endpoint"
level="information" vd="root" eventtime=1557847179037488154 logdesc="FortiClient connection
closed" action="close" status="success" license_limit="unlimited" used_for_type=5
connection_type="sslvpn" count=1 user="skubas" ip=172.18.64.250 name="VAN-200957-PC"
fctuid="52C66FE08F724FE0B116DAD5062C96CD" msg="Close a FortiClient Connection."
```

## Type and Subtype

### *Event Logs > HA Events*

#### Log configuration requirements

```
config log eventfilter
 set event enable
 set ha enable
end
```

#### Sample log

```
date=2019-05-10 time=09:53:21 logid="0108037892" type="event" subtype="ha" level="notice"
vd="root" eventtime=1557507201608871077 logdesc="Virtual cluster member state moved"
msg="Virtual cluster's member state moved" ha_role="master" vcluster=1 vcluster_state="work"
vcluster_member=0 hostname="FW_QA4" sn="FG2K5E3916900348"

date=2019-05-10 time=09:53:18 logid="0108037894" type="event" subtype="ha" level="critical"
vd="root" eventtime=1557507199208575235 logdesc="Virtual cluster member joined" msg="Virtual
cluster detected member join" vcluster=1 ha_group=0 sn="FG2K5E3916900286"
```

## Type and Subtype

### *Event Logs > Security Rating Events*

#### Log configuration requirements

```
config log eventfilter
 set event enable
 set security-rating enable
end
```

#### Sample log

```
date=2019-05-13 time=14:40:59 logid="0110052000" type="event" subtype="security-rating"
level="notice" vd="root" eventtime=1557783659536252389 logdesc="Security Rating summary"
auditid=1557783648 audittime=1557783659 auditscore="5.0" criticalcount=1 highcount=6
mediumcount=8 lowcount=0 passedcount=38
```

## Type and Subtype

### *Event Logs > WAN Opt & Cache Events*

#### Log configuration requirements

```
config log eventfilter
 set event enable
 set wan-opt enable
end
```

### Sample log

```
date=2019-05-14 time=09:37:46 logid="0105048039" type="event" subtype="wad" level="error"
vd="root" eventtime=1557851867382676560 logdesc="SSL fatal alert sent" session_id=0
policyid=0 srcip=0.0.0.0 srcport=0 dstip=208.91.113.83 dstport=636 action="send" alert="2"
desc="certificate unknown" msg="SSL Alert sent"
```

```
date=2019-05-10 time=15:48:31 logid="0105048038" type="event" subtype="wad" level="error"
vd="root" eventtime=1557528511221374615 logdesc="SSL Fatal Alert received" session_
id=5f88ddd1 policyid=0 srcip=172.18.70.15 srcport=59880 dstip=91.189.89.223 dstport=443
action="receive" alert="2" desc="unknown ca" msg="SSL Alert received"
```

### Type and Subtype

*Event Logs > Wireless*

#### Log configuration requirements

```
config log eventfilter
 set event enable
 set wireless-activity enable
end
```

```
config wireless-controller log
 set status enable
end
```

### Sample log

```
date=2019-05-13 time=11:30:08 logid="0104043568" type="event" subtype="wireless"
level="warning" vd="vdom1" eventtime=1557772208134721423 logdesc="Fake AP on air"
ssid="fortinet" bssid="90:6c:ac:89:e1:fa" aptype=0 rate=130 radioband="802.11n" channel=6
action="fake-ap-on-air" manuf="Fortinet, Inc." security="WPA2 Personal" encryption="AES"
signal=-93 noise=-95 live=353938 age=505 onwire="no" detectionmethod="N/A" stamac="N/A"
apscan="N/A" sndetected="N/A" radioiddetected=0 stacount=0 snclosest="FP320C3X17001909"
radioidclosest=0 apstatus=0 msg="Fake AP On-air fortinet 90:6c:ac:89:e1:fa chan 6 live
353938 age 505"
```

### Type and Subtype

*Event Logs > SDN Connector*

#### Log configuration requirements

```
config log eventfilter
 set event enable
 set connector enable
end
```

### Sample log

```
date=2019-05-13 time=16:09:43 logid="0112053200" type="event" subtype="connector"
level="information" vd="root" eventtime=1557788982 logdesc="IP address added" cfgobj="aws1"
```

```
action="object-add" addr="54.210.36.196" cldobjid="i-0fe5alef16bb94796" netid="vpc-97e81cee"
msg="connector object discovered in addr-obj aws1, 54.210.36.196"
```

```
date=2019-05-13 time=16:09:43 logid="0112053201" type="event" subtype="connector"
level="information" vd="root" eventtime=1557788982 logdesc="IP address removed"
cfgobj="aws1" action="object-remove" addr="172.31.31.101" cldobjid="i-0fe5alef16bb94796"
netid="vpc-97e81cee" msg="connector object removed in addr-obj aws1, 172.31.31.101"
```

## Type and Subtype

### Event Logs > FortiExtender Events

### Log configuration requirements

```
config log eventfilter
 set event enable
 set fortiextender enable
end
```

### Sample log

```
date=2019-02-20 time=09:57:22 logid="0111046400" type="event" subtype="fortiextender"
level="notice" vd="root" eventtime=1550685442 logdesc="FortiExtender system activity"
action="FortiExtender Authorized" msg="ext SN:FX04DN4N16002352 authorized"
```

```
date=2019-02-20 time=09:51:42 logid="0111046401" type="event" subtype="fortiextender"
level="notice" vd="root" eventtime=1550685102 logdesc="FortiExtender controller activity"
sn="FX04DN4N16002352" ip=11.11.11.2 action="ext session-deauthed" msg="ext
SN:FX04DN4N16002352 deauthorized"
```

```
date=2019-02-20 time=10:02:26 logid="0111046409" type="event" subtype="fortiextender"
level="information" vd="root" eventtime=1550685746 logdesc="Remote FortiExtender info
activity" sn="FX04DN4N16002352" ip=11.11.11.2 action="Cellular Connected"
imei="359376060442770" imsi="302720502331361" iccid="89302720403038146410"
phonenumber="+16045067526" carrier="Rogers" plan="Rogers-plan" apn="N/A" service="LTE"
msg="FX04DN4N16002352 STATE: sim with imsi:302720502331361 in slot:2 on carrier:Rogers
connected"
```

```
date=2019-02-20 time=10:33:57 logid="0111046407" type="event" subtype="fortiextender"
level="warning" vd="root" eventtime=1550687636 logdesc="Remote FortiExtender warning
activity" sn="FX04DN4N16002352" ip=11.11.11.2 action="Cellular Disconnected"
imei="359376060442770" imsi="N/A" iccid="N/A" phonenumber="N/A" carrier="N/A" plan="N/A"
apn="N/A" service="LTE" msg="FX04DN4N16002352 STATE: sim with imsi: in slot:2 on carrier:N/A
disconnected"
```

```
date=2019-02-20 time=10:02:24 logid="0111046409" type="event" subtype="fortiextender"
level="information" vd="root" eventtime=1550685744 logdesc="Remote FortiExtender info
activity" sn="FX04DN4N16002352" ip=11.11.11.2 action="Cellular Connecting"
imei="359376060442770" imsi="302720502331361" iccid="89302720403038146410"
phonenumber="+16045067526" carrier="Rogers" plan="Rogers-plan" apn="N/A" service="N/A"
msg="FX04DN4N16002352 STATE: sim with imsi:302720502331361 in slot:2 on carrier:Rogers
connecting"
```

```
date=2019-02-20 time=10:47:19 logid="0111046407" type="event" subtype="fortiextender"
level="warning" vd="root" eventtime=1550688438 logdesc="Remote FortiExtender warning
activity" sn="FX04DN4N16002352" ip=11.11.11.2 action="SIM Change" imei="N/A" slot=2
msg="FX04DN4N16002352 SIM: SIM2 is inserted"
```



```
date=2019-02-20 time=10:57:50 logid="0111046407" type="event" subtype="fortiextender"
level="warning" vd="root" eventtime=1550689069 logdesc="Remote FortiExtender warning
activity" sn="FX04DN4N16002352" ip=11.11.11.2 action="SIM Change" imei="359376060442770"
slot=1 msg="FX04DN4N16002352 SIM: SIM2 is plucked out"
```

```
date=2019-02-20 time=12:02:24 logid="0111046407" type="event" subtype="fortiextender"
level="warning" vd="root" eventtime=1550692942 logdesc="Remote FortiExtender warning
activity" sn="FX04DN4N16002352" ip=11.11.11.2 action="SIM Switch" imei="359376060442770"
reason="sim-switch can't take effect due to unavailability of 2 sim cards"
msg="FX04DN4N16002352 SIM: sim-switch can't take effect due to unavailability of 2 sim
cards"
```

```
date=2019-02-19 time=18:08:46 logid="0111046409" type="event" subtype="fortiextender"
level="information" vd="root" eventtime=1550628524 logdesc="Remote FortiExtender info
activity" sn="FX04DN4N16002352" ip=11.11.11.2 action="Cellular Signal Statistics"
imei="359376060442770" imsi="302720502331361" iccid="89302720403038146410"
phonenumber="+16045067526" carrier="Rogers" plan="Rogers-plan" service="LTE" sinr="7.0 dB"
rsrp="-89 dBm" rsrq="-16 dB" signalstrength="92 dBm" rssi="-54" temperature="40 C" apn="N/A"
msg="FX04DN4N16002352 INFO: LTE RSSI=-54dBm,RSRP=-89dBm,RSRQ=-
16dB,SINR=7.0dB,BAND=B2,CELLID=061C700F,BW=15MHz,RXCH=1025,TXCH=19025,TAC=8AAC,TEMPERATURE=4
0 C"
```

```
date=2019-02-19 time=18:09:46 logid="0111046409" type="event" subtype="fortiextender"
level="information" vd="root" eventtime=1550628585 logdesc="Remote FortiExtender info
activity" sn="FX04DN4N16002352" ip=11.11.11.2 action="Cellular Data Statistics"
imei="359376060442770" imsi="302720502331361" iccid="89302720403038146410"
phonenumber="+16045067526" carrier="Rogers" plan="Rogers-plan" service="LTE" rcvbyte=7760
sentbyte=3315 msg="FX04DN4N16002352 INFO: SIM2 LTE, rx=7760, tx=3315, rx_diff=2538, tx_
diff=567"
```

## Type and Subtype

### Security Logs > Antivirus

#### Log configuration requirements

```
config antivirus profile
 edit "test-av"
 config http
 set options scan
 end
 set av-virus-log enable
 set av-block-log enable
 next
end

config firewall policy
 edit 1
 set srcintf "port12"
 set dstintf "port11"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set utm-status enable
 set av-profile "test-av"
```

```

 set logtraffic utm
 set nat enable
next
end

```

## Sample log

```

date=2019-05-13 time=11:45:03 logid="0211008192" type="utm" subtype="virus"
eventtype="infected" level="warning" vd="vdom1" eventtime=1557773103767393505 msg="File is
infected." action="blocked" service="HTTP" sessionid=359260 srcip=10.1.100.11
dstip=172.16.200.55 srcport=60446 dstport=80 srcintf="port12" srcintfrole="undefined"
dstintf="port11" dstintfrole="undefined" policyid=4 proto=6 direction="incoming"
filename="eicar.com" quarskip="File-was-not-quarantined." virus="EICAR_TEST_FILE"
dtype="Virus" ref="http://www.fortinet.com/ve?vn=EICAR_TEST_FILE" virusid=2172
url="http://172.16.200.55/virus/eicar.com" profile="g-default" agent="curl/7.47.0"
analyticsscksum="275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f"
analyticssubmit="false" crscore=50 craction=2 crlevel="critical"

Corresponding Traffic Log
date=2019-05-13 time=11:45:04 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="vdom1" eventtime=1557773104815101919 srcip=10.1.100.11 srcport=60446
srcintf="port12" srcintfrole="undefined" dstip=172.16.200.55 dstport=80 dstintf="port11"
dstintfrole="undefined" srcuuid="48420c8a-5c88-51e9-0424-a37f9e74621e" dstuuid="187d6f46-
5c86-51e9-70a0-fadcfc349c3e" poluuid="3888b41a-5c88-51e9-cb32-1c32c66b4edf" sessionid=359260
proto=6 action="close" policyid=4 policytype="policy" service="HTTP" dstcountry="Reserved"
srccountry="Reserved"trandisp="snat" transip=172.16.200.2 transport=60446 appid=15893
app="HTTP.BROWSER" appcat="Web.Client" apprisk="medium" applist="g-default" duration=1
sentbyte=412 rcvdbyte=2286 sentpkt=6 rcvpkt=6 wanin=313 wanout=92 lanin=92 lanout=92
utmaction="block" countav=1 countapp=1 crscore=50 craction=2 osname="Ubuntu"
mastersrcmac="a2:e9:00:ec:40:01" srcmac="a2:e9:00:ec:40:01" srcserver=0 utmref=65497-770

```

## Type and Subtype

*Security Logs > Web Filter*

## Log configuration requirements

```

config webfilter profile
edit "test-webfilter"
 set web-content-log enable
 set web-filter-activex-log enable
 set web-filter-command-block-log enable
 set web-filter-cookie-log enable
 set web-filter-applet-log enable
 set web-filter-jscript-log enable
 set web-filter-js-log enable
 set web-filter-vbs-log enable
 set web-filter-unknown-log enable
 set web-filter-referer-log enable
 set web-filter-cookie-removal-log enable
 set web-url-log enable
 set web-invalid-domain-log enable
 set web-ftgd-err-log enable
 set web-ftgd-quota-usage enable
next
end

```

```
config firewall policy
 edit 1
 set name "v4-out"
 set srcintf "port12"
 set dstintf "port11"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set logtraffic utm
 set utm-status enable
 set webfilter-profile "test-webfilter"
 set nat enable
 next
end
```

## Sample log

```
date=2019-05-13 time=16:29:45 logid="0316013056" type="utm" subtype="webfilter"
eventtype="ftgd_blk" level="warning" vd="vdom1" eventtime=1557790184975119738 policyid=1
sessionid=381780 srcip=10.1.100.11 srcport=44258 srcintf="port12" srcintfrole="undefined"
dstip=185.244.31.158 dstport=80 dstintf="port11" dstintfrole="undefined" proto=6
service="HTTP" hostname="morrishittu.ddns.net" profile="test-webfilter" action="blocked"
reqtype="direct" url="/" sentbyte=84 rcvbyte=0 direction="outgoing" msg="URL belongs to a
denied category in policy" method="domain" cat=26 catdesc="Malicious Websites" crscore=30
craction=4194304 crlevel="high"
```

```
Corresponding traffic log
date=2019-05-13 time=16:29:50 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="vdom1" eventtime=1557790190452146185 srcip=10.1.100.11 srcport=44258
srcintf="port12" srcintfrole="undefined" dstip=185.244.31.158 dstport=80 dstintf="port11"
dstintfrole="undefined" srcuuid="ae28f494-5735-51e9-f247-d1d2ce663f4b" dstuuid="ae28f494-
5735-51e9-f247-d1d2ce663f4b" poluuid="ccb269e0-5735-51e9-a218-a397dd08b7eb" sessionid=381780
proto=6 action="close" policyid=1 policytype="policy" service="HTTP" dstcountry="Germany"
srccountry="Reserved" trandisp="snat" transip=172.16.200.2 transport=44258 duration=5
sentbyte=736 rcvbyte=3138 sentpkt=14 rcvdpkt=5 appcat="unscanned" utmaction="block"
countweb=1 crscore=30 craction=4194304 osname="Ubuntu" mastersrcmac="a2:e9:00:ec:40:01"
srcmac="a2:e9:00:ec:40:01" srcserver=0 utmref=65497-796
```

## Type and Subtype

*Security Logs > DNS Query*

### Log configuration requirements

```
config dnsfilter profile
 edit "dnsfilter_fgd"
 config ftgd-dns
 set options error-allow
 end
 set log-all-domain enable
 set block-botnet enable
 next
end
```

```
config firewall policy
 edit 1
 set srcintf "port12"
 set dstintf "port11"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set utm-status enable
 set dnsfilter-profile "dnsfilter_fgd"
 set logtraffic utm
 set nat enable
 next
end
```

## Sample log

```
date=2019-05-15 time=15:05:49 logid="1501054802" type="utm" subtype="dns" eventtype="dns-
response" level="notice" vd="vdom1" eventtime=1557957949740931155 policyid=1 sessionid=6887
srcip=10.1.100.22 srcport=50002 srcintf="port12" srcintfrole="undefined"
dstip=172.16.100.100 dstport=53 dstintf="port11" dstintfrole="undefined" proto=17
profile="dnsfilter_fgd" srcmac="a2:e9:00:ec:40:41" xid=57945 qname="changelogs.ubuntu.com"
qtype="AAAA" qtypeval=28 qclass="IN" ipaddr="2001:67c:1560:8008::11" msg="Domain is
monitored" action="pass" cat=52 catdesc="Information Technology"

date=2019-05-15 time=15:05:49 logid="1500054000" type="utm" subtype="dns" eventtype="dns-
query" level="information" vd="vdom1" eventtime=1557957949653103543 policyid=1
sessionid=6887 srcip=10.1.100.22 srcport=50002 srcintf="port12" srcintfrole="undefined"
dstip=172.16.100.100 dstport=53 dstintf="port11" dstintfrole="undefined" proto=17
profile="dnsfilter_fgd" srcmac="a2:e9:00:ec:40:41" xid=57945 qname="changelogs.ubuntu.com"
qtype="AAAA" qtypeval=28 qclass="IN"

Corresponding traffic log
date=2019-05-15 time=15:08:49 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="vdom1" eventtime=1557958129950003945 srcip=10.1.100.22 srcport=50002
srcintf="port12" srcintfrole="undefined" dstip=172.16.100.100 dstport=53 dstintf="port11"
dstintfrole="undefined" srcuid="ae28f494-5735-51e9-f247-d1d2ce663f4b" dstuid="ae28f494-
5735-51e9-f247-d1d2ce663f4b" poluid="ccb269e0-5735-51e9-a218-a397dd08b7eb" sessionid=6887
proto=17 action="accept" policyid=1 policytype="policy" service="DNS" dstcountry="Reserved"
srccountry="Reserved" trandisp="snat" transip=172.16.200.2 transport=50002 duration=180
sentbyte=67 rcvdbyte=207 sentpkt=1 rcvdpkt=1 appcat="unscanned" utmaction="allow" countdns=1
osname="Linux" mastersrcmac="a2:e9:00:ec:40:41" srcmac="a2:e9:00:ec:40:41" srcserver=0
utmref=65495-306
```

## Type and Subtype

*Security Logs > Application Control*

### Log configuration requirements

# log enabled by default in application profile entry

```
config application list
 edit "block-social.media"
```

```
 set other-application-log enable
 config entries
 edit 1
 set category 2 5 6 23
 set log enable
 next
 end
next
end

config firewall policy
 edit 1
 set name "to_Internet"
 set srcintf "port10"
 set dstintf "port9"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set utm-status enable
 set logtraffic utm
 set application-list "block-social.media"
 set ssl-ssh-profile "deep-inspection"
 set nat enable
 next
end
```

## Sample log

```
date=2019-05-15 time=18:03:36 logid="1059028704" type="utm" subtype="app-ctrl"
eventtype="app-ctrl-all" level="information" vd="root" eventtime=1557968615 appid=40568
srcip=10.1.100.22 dstip=195.8.215.136 srcport=50798 dstport=443 srcintf="port10"
srcintfrole="lan" dstintf="port9" dstintfrole="wan" proto=6 service="HTTPS"
direction="outgoing" policyid=1 sessionid=4414 applist="block-social.media"
appcat="Web.Client" app="HTTPS.BROWSER" action="pass" hostname="www.dailymotion.com"
incidentserialno=1962906680 url="/" msg="Web.Client: HTTPS.BROWSER," apprisk="medium"
scertcname="*.dailymotion.com" scertissuer="DigiCert SHA2 High Assurance Server CA"
```

```
date=2019-05-15 time=18:03:35 logid="1059028705" type="utm" subtype="app-ctrl"
eventtype="app-ctrl-all" level="warning" vd="root" eventtime=1557968615 appid=16072
srcip=10.1.100.22 dstip=195.8.215.136 srcport=50798 dstport=443 srcintf="port10"
srcintfrole="lan" dstintf="port9" dstintfrole="wan" proto=6 service="HTTPS"
direction="incoming" policyid=1 sessionid=4414 applist="block-social.media"
appcat="Video/Audio" app="Dailymotion" action="block" hostname="www.dailymotion.com"
incidentserialno=1962906682 url="/" msg="Video/Audio: Dailymotion," apprisk="elevated"
```

```
date=2019-05-15 time=18:03:35 logid="1059028705" type="utm" subtype="app-ctrl"
eventtype="app-ctrl-all" level="warning" vd="root" eventtime=1557968615 appid=16072
srcip=10.1.100.22 dstip=195.8.215.136 srcport=50798 dstport=443 srcintf="port10"
srcintfrole="lan" dstintf="port9" dstintfrole="wan" proto=6 service="HTTPS"
direction="incoming" policyid=1 sessionid=4414 applist="block-social.media"
appcat="Video/Audio" app="Dailymotion" action="block" hostname="www.dailymotion.com"
incidentserialno=1962906681 url="/" msg="Video/Audio: Dailymotion," apprisk="elevated"
```

```
Corresponding Traffic Log
```

```
date=2019-05-15 time=18:03:41 logid="0000000013" type="traffic" subtype="forward"
```

```
level="notice" vd="root" eventtime=1557968619 srcip=10.1.100.22 srcport=50798
srcintf="port10" srcintfrole="lan" dstip=195.8.215.136 dstport=443 dstintf="port9"
dstintfrole="wan" poluid="d8ce7a90-7763-51e9-e2be-741294c96f31" sessionid=4414 proto=6
action="client-rst" policyid=1 policytype="policy" service="HTTPS" dstcountry="France"
srccountry="Reserved" trandisp="snat" transip=172.16.200.10 transport=50798 appid=16072
app="Dailymotion" appcat="Video/Audio" apprisk="elevated" applist="block-social.media"
appact="drop-session" duration=5 sentbyte=1150 rcvdbyte=7039 sentpkt=13 utmaction="block"
countapp=3 devtype="Unknown" devcategory="None" mastersrcmac="00:0c:29:51:38:5e"
srcmac="00:0c:29:51:38:5e" srcserver=0 utmref=0-330
```

## Type and Subtype

*Security Logs > Intrusion Prevention*

### Log configuration requirements

```
log enabled by default in ips sensor

config ips sensor
 edit "block-critical-ips"
 config entries
 edit 1
 set severity critical
 set status enable
 set action block
 set log enable
 next
 end
 next
end

config firewall policy
 edit 1
 set name "to_Internet"
 set srcintf "port10"
 set dstintf "port9"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set utm-status enable
 set logtraffic utm
 set ips-sensor "block-critical-ips"
 set nat enable
 next
end
```

### Sample log

```
date=2019-05-15 time=17:56:41 logid="0419016384" type="utm" subtype="ips"
eventtype="signature" level="alert" vd="root" eventtime=1557968201 severity="critical"
srcip=10.1.100.22 srccountry="Reserved" dstip=172.16.200.55 srcintf="port10"
srcintfrole="lan" dstintf="port9" dstintfrole="wan" sessionid=4017 action="dropped" proto=6
service="HTTP" policyid=1 attack="Adobe.Flash.newfunction.Handling.Code.Execution"
```

```
srcport=46810 dstport=80 hostname="172.16.200.55" url="/ips/sig1.pdf" direction="incoming"
attackid=23305 profile="block-critical-ips" ref="http://www.fortinet.com/ids/VID23305"
incidentserialno=582633933 msg="applications3:
Adobe.Flash.newfunction.Handling.Code.Execution," crscore=50 craction=4096
crlevel="critical"
```

```
Corresponding Traffic Log
date=2019-05-15 time=17:58:10 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="root" eventtime=1557968289 srcip=10.1.100.22 srcport=46810
srcintf="port10" srcintfrole="lan" dstip=172.16.200.55 dstport=80 dstintf="port9"
dstintfrole="wan" poluid="d8ce7a90-7763-51e9-e2be-741294c96f31" sessionid=4017 proto=6
action="close" policyid=1 policytype="policy" service="HTTP" dstcountry="Reserved"
srccountry="Reserved" trandisp="snat" transip=172.16.200.10 transport=46810 duration=89
sentbyte=565 rcvdbyte=9112 sentpkt=9 rcvdpkt=8 appcat="unscanned" utmaction="block"
countips=1 crscore=50 craction=4096 devtype="Unknown" devcategory="None"
mastersrcmac="00:0c:29:51:38:5e" srcmac="00:0c:29:51:38:5e" srcserver=0 utmref=0-302
```

## Type and Subtype

*Security Logs > Anomaly*

### Log configuration requirements

```
config firewall DoS-policy
 edit 1
 set interface "port12"
 set srcaddr "all"
 set dstaddr "all"
 set service "ALL"
 config anomaly
 edit "icmp_flood"
 set status enable
 set log enable
 set action block
 set threshold 50
 next
 end
 next
end
```

### Sample log

```
date=2019-05-13 time=17:05:59 logid="0720018433" type="utm" subtype="anomaly"
eventtype="anomaly" level="alert" vd="vdom1" eventtime=1557792359461869329
severity="critical" srcip=10.1.100.11 srccountry="Reserved" dstip=172.16.200.55
srcintf="port12" srcintfrole="undefined" sessionid=0 action="clear_session" proto=1
service="PING" count=1 attack="icmp_flood" icmpid="0x1474" icmptype="0x08" icmpcode="0x00"
attackid=16777316 policyid=1 policytype="DoS-policy"
ref="http://www.fortinet.com/ids/VID16777316" msg="anomaly: icmp_flood, 51 > threshold 50"
crscore=50 craction=4096 crlevel="critical"
```

## Type and Subtype

*Security Logs > Data Leak Prevention*

## Log configuration requirements

```
config dlp sensor
 edit "dlp-file-type-test"
 set comment ''
 set replacemsg-group ''
 config filter
 edit 1
 set name ''
 set severity medium
 set type file
 set proto http-get http-post ftp
 set filter-by file-type
 set file-type 1
 set archive enable
 set action block
 next
 end
 set dlp-log enable
 next
end

config firewall policy
 edit 1
 set name "to_Internet"
 set srcintf "port10"
 set dstintf "port9"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set utm-status enable
 set inspection-mode proxy
 set logtraffic utm
 set dlp-sensor "dlp-file-type-test"
 set ssl-ssh-profile "deep-inspection"
 set nat enable
 next
end
```

## Sample log

```
date=2019-05-15 time=17:45:30 logid="0954024576" type="utm" subtype="dlp" eventtype="dlp"
level="warning" vd="root" eventtime=1557967528 filteridx=1 dlpextra="dlp-file-size11"
filtertype="file-type" filtercat="file" severity="medium" policyid=1 sessionid=3423
epoch=1740880646 eventid=0 srcip=10.1.100.22 srcport=50354 srcintf="port10"
srcintfrole="lan" dstip=52.216.177.83 dstport=443 dstintf="port9" dstintfrole="wan" proto=6
service="HTTPS" filetype="pdf" direction="incoming" action="block"
hostname="fortinetweb.s3.amazonaws.com" url="/docs.fortinet.com/v2/attachments/be3d0e3d-
4b62-11e9-94bf-00505692583a/FortiOS_6.2.0_Log_Reference.pdf" agent="Wget/1.17.1"
filename="FortiOS_6.2.0_Log_Reference.pdf" filesize=16360 profile="dlp-file-type-test"

Corresponding Traffic Log
date=2019-05-15 time=17:45:34 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="root" eventtime=1557967534 srcip=10.1.100.22 srcport=50354
srcintf="port10" srcintfrole="lan" dstip=52.216.177.83 dstport=443 dstintf="port9"
```



```
dstintfrole="wan" poluuid="d8ce7a90-7763-51e9-e2be-741294c96f31" sessionid=3423 proto=6
action="server-rst" policyid=1 policytype="policy" service="HTTPS" dstcountry="United
States" srccountry="Reserved" trandisp="snat" transip=172.16.200.10 transport=50354
duration=5 sentbyte=2314 rcvbyte=5266 sentpkt=33 rcvpkt=12 appcat="unscanned" wanin=43936
wanout=710 lanin=753 lanout=753 utmaction="block" countdlp=1 crscore=5 craction=262144
crlevel="low" devtype="Unknown" devcategory="None" mastersrcmac="00:0c:29:51:38:5e"
srcmac="00:0c:29:51:38:5e" srcserver=0 utmref=0-152
```

## Type and Subtype

*Security Logs > SSH*

*Security Logs > SSL*

### Log configuration requirements

```
config ssh-filter profile
 edit "ssh-deepscan"
 set block shell
 set log shell
 set default-command-log disable
 next
end

config firewall policy
 edit 1
 set srcintf "port21"
 set dstintf "port23"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set utm-status enable
 set inspection-mode proxy
 set ssh-filter-profile "ssh-deepscan"
 set profile-protocol-options "protocol"
 set ssl-ssh-profile "ssl"
 set nat enable
 next
end
```

### For SSL-Traffic-log, enable logtraffic all

```
config firewall policy
 edit 1
 set srcintf "dmz"
 set dstintf "wan1"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set utm-status enable
 set inspection-mode proxy
 set logtraffic all
```

```
 set ssl-ssh-profile "deep-inspection"
 set nat enable
 next
end
```

## For SSL-UTM-log

```
#EVENTTYPE="SSL-ANOMALIES"
```

By default, `ssl-anomalies-log` is enabled.

```
config firewall ssl-ssh-profile
 edit "deep-inspection"
 set comment "Read-only deep inspection profile."
 set server-cert-mode re-sign
 set caname "Fortinet_CA_SSL"
 set untrusted-caname "Fortinet_CA_Untrusted"
 set ssl-anomalies-log enable
 set ssl-exemptions-log disable
 set rpc-over-https disable
 set mapi-over-https disable
 set use-ssl-server disable
 next
end

EVENTTYPE="SSL-EXEMPT"
```

Need to enable `ssl-exemptions-log` to generate `ssl-utm-exempt` log.

```
config firewall ssl-ssh-profile
 edit "deep-inspection"
 set comment "Read-only deep inspection profile."
 set server-cert-mode re-sign
 set caname "Fortinet_CA_SSL"
 set untrusted-caname "Fortinet_CA_Untrusted"
 set ssl-anomalies-log enable
 set ssl-exemptions-log enable
 set rpc-over-https disable
 set mapi-over-https disable
 set use-ssl-server disable
 next
end
```

## Sample log for SSH

```
date=2019-05-15 time=16:18:17 logid="1601061010" type="utm" subtype="ssh" eventtype="ssh-channel" level="warning" vd="vdom1" eventtime=1557962296 policyid=1 sessionid=344 profile="ssh-deepscan" srcip=10.1.100.11 srcport=43580 dstip=172.16.200.44 dstport=22 srcintf="port21" srcintfrole="undefined" dstintf="port23" dstintfrole="undefined" proto=6 action="blocked" direction="outgoing" login="root" channeltype="shell"
```

```
Corresponding Traffic Log
```

```
date=2019-05-15 time=16:18:18 logid="0000000013" type="traffic" subtype="forward" level="notice" vd="vdom1" eventtime=1557962298 srcip=10.1.100.11 srcport=43580 srcintf="port21" srcintfrole="undefined" dstip=172.16.200.44 dstport=22 dstintf="port23" dstintfrole="undefined" poluid="49871fae-7371-51e9-17b4-43c7ff119195" sessionid=344 proto=6 action="close" policyid=1 policytype="policy" service="SSH" dstcountry="Reserved" srccountry="Reserved" trandisp="snat" transip=172.16.200.171 transport=43580 duration=8
```

```
sentbyte=3093 rcvdbyte=2973 sentpkt=18 rcvpkt=16 appcat="unscanned" utmaction="block"
countssh=1 utmref=65535-0
```

## Sample log for SSL

### For SSL-Traffic-log

```
date=2019-05-16 time=10:08:26 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="root" eventtime=1558026506763925658 srcip=10.1.100.66 srcport=38572
srcintf="dmz" srcintfrole="dmz" dstip=104.154.89.105 dstport=443 dstintf="wan1"
dstintfrole="wan" poluid="a17c0a38-75c6-51e9-4c0d-d547347b63e5" sessionid=100 proto=6
action="server-rst" policyid=1 policytype="policy" service="HTTPS" dstcountry="United
States" srccountry="Reserved" trandisp="snat" transip=172.16.200.11 transport=38572
duration=5 sentbyte=930 rcvdbyte=6832 sentpkt=11 rcvpkt=19 appcat="unscanned" wanin=1779
wanout=350 lanin=754 lanout=754 utmaction="block" countssl=1 crscore=5 craction=262144
crlevel="low" utmref=65467-0
```

### For SSL-UTM-log

```
#EVENTTYPE="SSL-ANOMALIES"
```

```
date=2019-03-28 time=10:44:53 logid="1700062002" type="utm" subtype="ssl" eventtype="ssl-
anomalies" level="warning" vd="vdom1" eventtime=1553795092 policyid=1 sessionid=10796
service="HTTPS" srcip=10.1.100.66 srcport=43602 dstip=104.154.89.105 dstport=443
srcintf="port2" srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" proto=6
action="blocked" msg="Server certificate blocked" reason="block-cert-invalid"
```

```
date=2019-03-28 time=10:51:17 logid="1700062002" type="utm" subtype="ssl" eventtype="ssl-
anomalies" level="warning" vd="vdom1" eventtime=1553795476 policyid=1 sessionid=11110
service="HTTPS" srcip=10.1.100.66 srcport=49076 dstip=172.16.200.99 dstport=443
srcintf="port2" srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" proto=6
action="blocked" msg="Server certificate blocked" reason="block-cert-untrusted"
```

```
date=2019-03-28 time=10:55:43 logid="1700062002" type="utm" subtype="ssl" eventtype="ssl-
anomalies" level="warning" vd="vdom1" eventtime=1553795742 policyid=1 sessionid=11334
service="HTTPS" srcip=10.1.100.66 srcport=49082 dstip=172.16.200.99 dstport=443
srcintf="port2" srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" proto=6
action="blocked" msg="Server certificate blocked" reason="block-cert-req"
```

```
date=2019-03-28 time=10:57:42 logid="1700062053" type="utm" subtype="ssl" eventtype="ssl-
anomalies" level="warning" vd="vdom1" eventtime=1553795861 policyid=1 sessionid=11424
service="SMTPS" profile="block-unsupported-ssl" srcip=10.1.100.66 srcport=41296
dstip=172.16.200.99 dstport=8080 srcintf="port2" srcintfrole="undefined" dstintf=unknown-0
dstintfrole="undefined" proto=6 action="blocked" msg="Connection is blocked due to
unsupported SSL traffic" reason="malformed input"
```

```
date=2019-03-28 time=11:00:17 logid="1700062002" type="utm" subtype="ssl" eventtype="ssl-
anomalies" level="warning" vd="vdom1" eventtime=1553796016 policyid=1 sessionid=11554
service="HTTPS" srcip=10.1.100.66 srcport=49088 dstip=172.16.200.99 dstport=443
srcintf="port2" srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" proto=6
action="blocked" msg="Server certificate blocked" reason="block-cert-sni-mismatch"
```

```
date=2019-03-28 time=11:02:07 logid="1700062000" type="utm" subtype="ssl" eventtype="ssl-
anomalies" level="warning" vd="vdom1" eventtime=1553796126 policyid=1 sessionid=11667
service="HTTPS" srcip=10.1.100.66 srcport=49096 dstip=172.16.200.99 dstport=443
srcintf="port2" srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" proto=6
```

```
action="blocked" msg="Certificate blocklisted"
certhash="1115ec1857ed7f937301ff5e02f6b0681cf2ec4e" reason="Other"

EVENTTYPE="SSL-EXEMPT"

date=2019-03-28 time=11:06:05 logid="1701062003" type="utm" subtype="ssl" eventtype="ssl-
exempt" level="notice" vd="vdom1" eventtime=1553796363 policyid=1 sessionid=11871
service="HTTPS" srcip=10.1.100.66 srcport=47384 dstip=50.18.221.132 dstport=443
srcintf="port2" srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" proto=6
action="exempt" msg="SSL connection exempted" reason="exempt-whitelist"

date=2019-03-28 time=11:09:14 logid="1701062003" type="utm" subtype="ssl" eventtype="ssl-
exempt" level="notice" vd="vdom1" eventtime=1553796553 policyid=1 sessionid=12079
service="HTTPS" srcip=10.1.100.66 srcport=49102 dstip=172.16.200.99 dstport=443
srcintf="port2" srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" proto=6
action="exempt" msg="SSL connection exempted" reason="exempt-addr"

date=2019-03-28 time=11:10:55 logid="1701062003" type="utm" subtype="ssl" eventtype="ssl-
exempt" level="notice" vd="vdom1" eventtime=1553796654 policyid=1 sessionid=12171
service="HTTPS" srcip=10.1.100.66 srcport=47390 dstip=50.18.221.132 dstport=443
srcintf="port2" srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" proto=6
action="exempt" msg="SSL connection exempted" reason="exempt-ftgd-cat"
```

## Type and Subtype

### Security Logs > CIFS

#### Log configuration requirements

```
config cifs profile
 edit "cifs"
 set server-credential-type none
 config file-filter
 set status enable
 set log enable
 config entries
 edit "1"
 set comment ''
 set action block
 set direction any
 set file-type "msoffice"
 next
 end
 end
next
end

config firewall policy
 edit 1
 set srcintf "port21"
 set dstintf "port23"
 set srcaddr "all"
 set dstaddr "all"
 set action accept
 set schedule "always"
 set service "ALL"
 set utm-status enable
```

```
set inspection-mode proxy
set cifs-profile "cifs"
set profile-protocol-options "protocol"
set ssl-ssh-profile "ssl"
set nat enable
next
end
```

### Sample log

```
date=2019-05-15 time=16:28:17 logid="1800063000" type="utm" subtype="cifs" eventtype="cifs-
filefilter" level="warning" vd="vdom1" eventtime=1557962895 msg="File was blocked by file
filter." direction="incoming" action="blocked" service="CIFS" srcip=10.1.100.11
dstip=172.16.200.44 srcport=56348 dstport=445 srcintf="port21" srcintfrole="undefined"
dstintf="port23" dstintfrole="undefined" policyid=1 proto=16 profile="cifs" filesize="13824"
filename="sample\\test.xls" filtername="1" filetype="msoffice"
```

## Checking the email filter log

### To check the email filter log in the CLI:

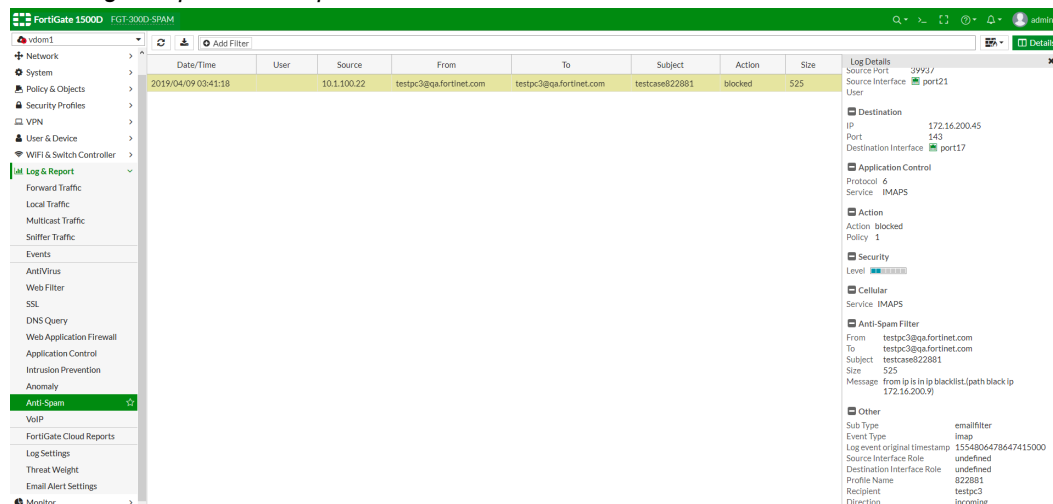
```
execute log filter category 5
```

```
execute log display
1 logs found.
1 logs returned.
```

```
1: date=2019-04-09 time=03:41:18 logid="0510020491" type="utm" subtype="emailfilter"
eventtype="imap" level="notice" vd="vdom1" eventtime=1554806478647415130 policyid=1
sessionid=439 srcip=10.1.100.22 srcport=39937 srcintf="port21" srcintfrole="undefined"
dstip=172.16.200.45 dstport=143 dstintf="port17" dstintfrole="undefined" proto=6
service="IMAPS" profile="822881" action="blocked" from="testpc3@qa.fortinet.com"
to="testpc3@qa.fortinet.com" recipient="testpc3" direction="incoming" msg="from ip is in ip
blocklist.(path block ip 172.16.200.9)" subject="testcase822881" size="525" attachment="no"
```

## To check the email filter log in the GUI:

### 1. Go to *Log & Report > Anti-Spam*.



## Supported log types to FortiAnalyzer, FortiAnalyzer Cloud, FortiGate Cloud, and syslog

FortiGate supports sending logs of all log types to FortiAnalyzer, FortiGate Cloud, and Syslog. For FortiGates with a standard FortiAnalyzer Cloud subscription (FAZC contract), traffic logs are not sent to FortiAnalyzer Cloud; for FortiGates with a Premium subscription (AFAC contract), all logs are sent.

## Configuring multiple FortiAnalyzers on a multi-VDOM FortiGate

This topic shows a sample configuration of multiple FortiAnalyzers on a multi-VDOM FortiGate.

In this example:

- The FortiGate has three VDOMs:
  - Root (management VDOM)
  - VDOM1
  - VDOM2

- There are four FortiAnalyzers.

These IP addresses are used as examples in the instructions below.

- FAZ1: 172.16.200.55
- FAZ2: 172.18.60.25
- FAZ3: 192.168.1.253
- FAZ4: 192.168.1.254

- Set up FAZ1 and FAZ2 under global.
  - These two collect logs from the root VDOM and VDOM2.
  - FAZ1 and FAZ2 must be accessible from management VDOM root.
- Set up FAZ3 and FAZ4 under VDOM1.
  - These two collect logs from VDOM1.
  - FAZ3 and FAZ4 must be accessible from VDOM1.

### To set up FAZ1 as global FortiAnalyzer 1 from the GUI:

Prerequisite: FAZ1 must be reachable from the management root VDOM.

1. Go to *Global > Log & Report > Log Settings*.
2. Enable *Send logs to FortiAnalyzer/FortiManager*.
3. Enter the FortiAnalyzer IP.  
In this example: 172.16.200.55.
4. For *Upload option*, select *Real Time*.
5. Click *Apply*.

### To set up FAZ2 as global FortiAnalyzer 2 from the CLI:

Prerequisite: FAZ2 must be reachable from the management root VDOM.

```
config log fortianalyzer2 setting
 set status enable
 set server "172.18.60.25"
 set upload-option realtime
end
```

### To set up FAZ3 and FAZ4 as VDOM1 FortiAnalyzer 1 and FortiAnalyzer 2:

Prerequisite: FAZ3 and FAZ4 must be reachable from VDOM1.

```
config log setting
 set faz-override enable
end
```

```
config log fortianalyzer override-setting
 set status enable
 set server "192.168.1.253"
 set upload-option realtime
end
```

```
config log fortianalyzer2 override-setting
 set status enable
 set server "192.168.1.254"
 set upload-option realtime
end
```

## Checking FortiAnalyzer connectivity

To use the diagnose command to check FortiAnalyzer connectivity:

### 1. Check the global FortiAnalyzer status:

```
FGTA(global) # diagnose test application miglogd 1
faz: global , enabled
 server=172.16.200.55, realtime=3, ssl=1, state=connected, src=, mgmt_name=FGh_
Log_root_172.16.200.55, reliable=1
 status: ver=6, used_disk=0, total_disk=0, global=0, vfid=0 conn_
verified=N
 SNs: last sn update:1369 seconds ago.
 Sn list:

 queue: qlen=0.
filter: severity=6, sz_exclude_list=0
 voip dns ssh ssl
subcategory:
 traffic: forward local multicast sniffer
 anomaly: anomaly

 server: global, id=0, fd=90, ready=1, ipv6=0, 172.16.200.55/514
 oftp-state=5
faz2: global , enabled
 server=172.18.60.25, realtime=1, ssl=1, state=connected, src=, mgmt_name=FGh_
Log_root_172.18.60.25, reliable=0
 status: ver=6, used_disk=0, total_disk=0, global=0, vfid=0 conn_
verified=N
 SNs: last sn update:1369 seconds ago.
 Sn list:

 queue: qlen=0.
filter: severity=6, sz_exclude_list=0
 voip dns ssh ssl
subcategory:
 traffic: forward local multicast sniffer
 anomaly: anomaly

 server: global, id=1, fd=95, ready=1, ipv6=0, 172.18.60.25/514
 oftp-state=5
```

### 2. Check the VDOM1 override FortiAnalyzer status:

```
FGTA(global) # diagnose test application miglogd 3101
faz: vdom, enabled, override
 server=192.168.1.253, realtime=1, ssl=1, state=connected, src=, mgmt_name=FGh_
Log_root_192.168.1.253, reliable=1
 status: ver=6, used_disk=0, total_disk=0, global=0, vfid=0 conn_
verified=N
 SNs: last sn update:1369 seconds ago.
 Sn list:
 (FAZ-VM0000000001,age=17s)
 queue: qlen=0.
filter: severity=6, sz_exclude_list=0
 voip dns ssh ssl
subcategory:
```



```
traffic: forward local multicast sniffer
anomaly: anomaly

server: vdom, id=0, fd=72, ready=1, ipv6=0, 192.168.1.253/514
ofstp-state=5
faz2: vdom, enabled, override
 server=192.168.1.254, realtime=1, ssl=1, state=connected, src=, mgmt_name=FGh_
Log_root_192.168.1.254, reliable=0
 status: ver=6, used_disk=0, total_disk=0, global=0, vfid=0 conn_
verified=N
 SNs: last sn update:1369 seconds ago.
 Sn list:
 (FL-1KET318000008,age=17s)
 queue: qlen=0.
filter: severity=6, sz_exclude_list=0
 voip dns ssh ssl
subcategory:
 traffic: forward local multicast sniffer
 anomaly: anomaly

server: vdom, id=1, fd=97, ready=1, ipv6=0, 192.168.1.254/514
ofstp-state=5
faz3: vdom, disabled, override
```

## Configuring multiple FortiAnalyzers (or syslog servers) per VDOM

In a VDOM, multiple FortiAnalyzer and syslog servers can be configured as follows:

- Up to three override FortiAnalyzer servers
- Up to four override syslog servers

If the VDOM `faz-override` and/or `syslog-override` setting is enabled or disabled (default) before upgrading, the setting remains the same after upgrading.

If the override setting is disabled, the GUI displays the global FortiAnalyzer1 or syslog1 setting. If the override setting is enabled, the GUI displays the VDOM override FortiAnalyzer1 or syslog1 setting.

You can only use CLI to enable the override to support multiple log servers.

### To enable FortiAnalyzer and syslog server override under VDOM:

```
config log setting
 set faz-override enable
 set syslog-override enable
end
```

When `faz-override` and/or `syslog-override` is enabled, the following CLI commands are available for configuring VDOM override:

**To configure VDOM override for FortiAnalyzer:****1. Configure the FortiAnalyzer override settings:**

```
config log fortianalyzer/fortianalyzer2/fortianalyzer3 override-setting
 set status enable
 set server "123.12.123.123"
 set reliable enable
end
```

**2. Configure the override filters:**

```
config log fortianalyzer/fortianalyzer2/fortianalyzer3 override-filter
 set severity information
 set forward-traffic enable
 set local-traffic enable
 set multicast-traffic enable
 set sniffer-traffic enable
 set anomaly enable
 set voip enable
 set dlp-archive enable
 set dns enable
 set ssh enable
 set ssl enable
end
```

**To configure VDOM override for a syslog server:****1. Configure the syslog override settings:**

```
config log syslogd/syslogd2/syslogd3/syslogd4 override-setting
 set status enable
 set server "123.12.123.12"
 set facility local1
end
```

**2. Configure the override filters:**

```
config log syslogd/syslogd2/syslogd3/syslogd4 override-filter
 set severity information
 set forward-traffic enable
 set local-traffic enable
 set multicast-traffic enable
 set sniffer-traffic enable
 set anomaly enable
 set voip enable
 set dns enable
 set ssh enable
 set ssl enable
end
```

## Source and destination UUID logging

The `log-uuid` setting in `system global` is split into two settings: `log-uuid-address` and `log-uuid policy`.

The traffic log includes two `internet-service` name fields: *Source Internet Service* (`srcinetsvc`) and *Destination Internet Service* (`dstinetsvc`).

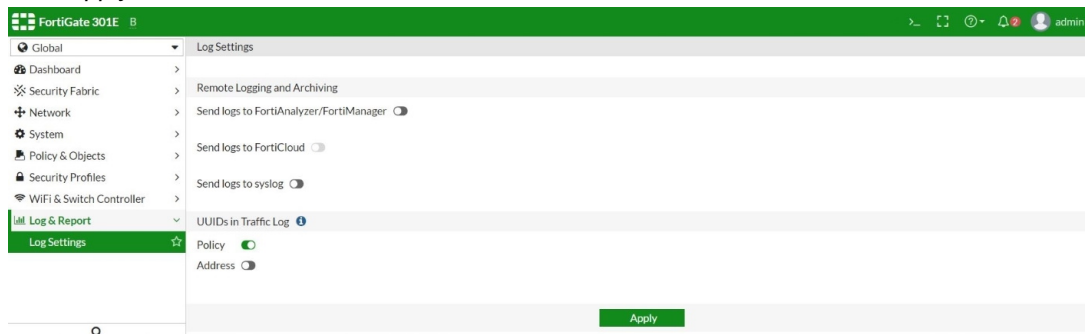
## Log UUIDs

UUIDs can be matched for each source and destination that match a policy that is added to the traffic log. This allows the address objects to be referenced in log analysis and reporting.

As this may consume a significant amount of storage space, this feature is optional. By default, policy UUID insertion is enabled and address UUID insertion is disabled.

### To enable address and policy UUID insertion in traffic logs using the GUI:

1. Go to *Log & Report > Log Settings*.
2. Under *UUIDs in Traffic Log*, enable *Policy* and/or *Address*.
3. Click *Apply*.



### To enable address and policy UUID insertion in traffic logs using the CLI:

```
config system global
 set log-uuid-address enable
 set log-uuid-policy enable
end
```

### Sample forward traffic log:

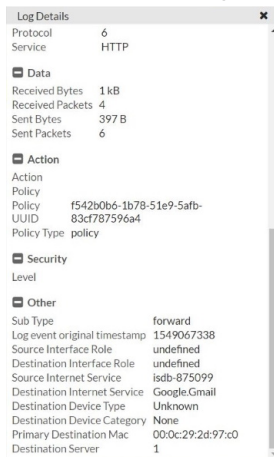
```
date=2019-01-25 time=11:32:55 logid="0000000013" type="traffic" subtype="forward"
 level="notice" vd="vdom1" eventtime=1528223575 srcip=192.168.1.183 srcname="PC24"
 srcport=33709 srcintf="lan" srcintfrole="lan" dstip=192.168.70.184 dstport=80
 dstintf="wan1" dstintfrole="wan" srcuuid="27dd503e-883c-51e7-ade1-7e015d46494f"
 dstuuid="27dd503e-883c-51e7-ade1-7e015d46494f"
 poluuid="9e0fe24c-1808-51e8-1257-68ce4245572c" sessionid=5181 proto=6
 action="client-rst" policyid=4 policytype="policy" service="HTTP" trandisp="snat"
 transip=192.168.70.228 transport=33709 appid=38783 app="Wget"
 appcat="General.Interest" apprisk="low" applist="default" duration=5 sentbyte=450
 rcvdbyte=2305 sentpkt=6 wanin=368 wanout=130 lanin=130 lanout=130 utmaction="block"
 countav=2 countapp=1 crscore=50 craction=2 devtype="Linux PC" devcategory="None"
 osname="Linux" mastersrcmac="00:0c:29:36:5c:c3" srcmac="00:0c:29:36:5c:c3"
 srcserver=0 utmref=65523-1018
```

## Internet service name fields

Traffic logs for `internet-service` include two fields: *Source Internet Service* and *Destination Internet Service*.

### To view the internet-service fields using the GUI:

1. Go to *Log & Report > Forward Traffic*.
2. Double-click on an entry to view the *Log Details*. The *Source Internet Service* and *Destination Internet Service* fields are visible in the *Log Details* pane.



Sample internet-service name fields in a forward traffic log:

```
date=2019-01-25 time=14:17:04 logid="0000000013" type="traffic" subtype="forward"
 level="notice" vd="vdom1" eventtime=1548454622 srcip=10.1.100.11 srcport=51112
 srcintf="port3" srcintfrole="undefined" dstip=172.217.14.228 dstport=80
 dstintf="port1" dstintfrole="undefined" poluuid="af519380-2094-51e9-391c-
 b78e8edbdfc" srcinetsvc="isdb-875099" dstinetsvc="Google.Gmail" sessionid=6930
 proto=6 action="close" policyid=2 policytype="policy" service="HTTP"
 dstcountry="United States" srccountry="Reserved" trandisp="snat"
 transip=172.16.200.2 transport=51112 duration=11 sentbyte=398 rcvdbyte=756 sentpkt=6
 rcvdpkt=4 appcat="unscanned" devtype="Router/NAT Device" devcategory="Fortinet
 Device" mastersrcmac="90:6c:ac:41:7a:24" srcmac="90:6c:ac:41:7a:24" srcserver=0
 dstdevtype="Unknown" dstdevcategory="Fortinet Device"
 masterdstmac="08:5b:0e:1f:ed:ed" dstmac="08:5b:0e:1f:ed:ed" dstserver=0
```

## Troubleshooting

The following topics provide information about troubleshooting logging and reporting:

- [Log-related diagnose commands on page 1646](#)
- [Backing up log files or dumping log messages on page 1652](#)
- [SNMP OID for logs that failed to send on page 1654](#)

## Log-related diagnose commands

This topic shows commonly used examples of log-related diagnose commands.

Use the following diagnose commands to identify log issues:

- The following commands enable debugging log daemon (miglogd) at the proper debug level:

```
diagnose debug application miglogd x
diagnose debug enable
```

- The following commands display different status/statistics of miglogd at the proper level:

```
diagnose test application miglogd x
diagnose debug enable
```

To get the list of available levels, press Enter after `diagnose test/debug application miglogd`. The following are some examples of commonly use levels.

If the debug log display does not return correct entries when log filter is set:

```
diagnose debug application miglogd 0x1000
```

For example, use the following command to display all login system event logs:

```
execute log filter device disk
execute log filter category event
execute log filter field action login
```

```
execute log display
```

Files to be searched:

```
file_no=65523, start line=0, end_line=237
file_no=65524, start line=0, end_line=429
file_no=65525, start line=0, end_line=411
file_no=65526, start line=0, end_line=381
file_no=65527, start line=0, end_line=395
file_no=65528, start line=0, end_line=458
file_no=65529, start line=0, end_line=604
file_no=65530, start line=0, end_line=389
file_no=65531, start line=0, end_line=384
session ID=1, total logs=3697
back ground search. process ID=26240, session_id=1
 start line=1 view line=10
(action "login")
ID=1, total=3697, checked=238, found=5
ID=1, total=3697, checked=668, found=13
ID=1, total=3697, checked=1080, found=23
ID=1, total=3697, checked=1462, found=23
ID=1, total=3697, checked=1858, found=23
ID=1, total=3697, checked=2317, found=54
ID=1, total=3697, checked=2922, found=106
ID=1, total=3697, checked=3312, found=111
ID=1, total=3697, checked=3697, found=114
```

You can check and/or debug the FortiGate to FortiAnalyzer connection status.

**To show connect status with detailed information:**

```
diagnose test application miglogd 1
```

```
faz: global , enabled
 server=172.18.64.234, realtime=3, ssl=1, state=connected, src=, mgmt_name=FGh_Log_
vdom1_172.18.64.234, reliable=0, sni_prefix_type=none, required_entitlement=none
 status: ver=6, used_disk=0, total_disk=0, global=0, vfid=0 conn_verified=Y
```

```
 SNs: last sn update:107 seconds ago.
 Sn list:
 (FL-8HFT718900132,age=107s)
 queue: qlen=0.
filter: severity=6, sz_exclude_list=0
 voip dns ssh ssl cifs
subcategory:
 traffic: forward local multicast sniffer
 anomaly: anomaly

 server: global, id=0, fd=132, ready=1, ipv6=0, 172.18.64.234/514
 oftp-state=5
```

**To collect debug information when FortiAnalyzer is enabled:**

```
diagnose debug application miglogd 0x100
```

```
FGT-B-LOG (global) # <16208> miglog_start_rmt_conn()-1552: setting epoll_hd:0x7fc364e125e0
to _rmt_connect
<16209> miglog_start_rmt_conn()-1552: setting epoll_hd:0x7f72647715e0 to _rmt_connect
<16206> miglog_start_rmt_conn()-1552: setting epoll_hd:0x141f69e0 to _rmt_connect
<16209> _rmt_connect()-1433: oftp is ready.
<16209> _rmt_connect()-1435: xfer_status changed from 2 to 2 for global-faz
<16209> _rmt_connect()-1439: setting epoll_hd:0x7f72647715e0 to _rmt_rcv
<16209> _check_oftp_certificate()-248: checking sn:FL-8HFT718900132 vs cert sn:FL-
8HFT718900132
<16209> _check_oftp_certificate()-252: Verified the certificate of peer (172.18.64.234) to
match sn=FL-8HFT718900132
<16209> _faz_post_connection()-292: Certificate verification:enabled, Faz verified:1
<16209> _send_queue_item()-518: xfer_status changed from 2 to 1 for global-faz
<16209> _send_queue_item()-523: type=0, cat=0, logcount=0, len=0
<16209> _oftp_send()-487: dev=global-faz type=17 pkt_len=34

<16209> _oftp_send()-487: opt=253, opt_len=10
<16209> _oftp_send()-487: opt=81, opt_len=12
<16208> _rmt_connect()-1433: oftp is ready.
<16208> _rmt_connect()-1435: xfer_status changed from 2 to 2 for global-faz
<16208> _rmt_connect()-1439: setting epoll_hd:0x7fc364e125e0 to _rmt_rcv
<16208> _check_oftp_certificate()-248: checking sn:FL-8HFT718900132 vs cert sn:FL-
8HFT718900132
<16208> _check_oftp_certificate()-252: Verified the certificate of peer (172.18.64.234) to
match sn=FL-8HFT718900132
<16208> _faz_post_connection()-292: Certificate verification:enabled, Faz verified:1
<16208> _send_queue_item()-518: xfer_status changed from 2 to 1 for global-faz
<16208> _send_queue_item()-523: type=0, cat=0, logcount=0, len=0
<16208> _oftp_send()-487: dev=global-faz type=17 pkt_len=34

<16208> _oftp_send()-487: opt=253, opt_len=10
<16209> _oftp_rcv()-1348: opt=252, opt_len=996
<16208> _oftp_send()-487: opt=81, opt_len=12
<16209> _process_response()-960: checking opt code=252
<16209> _faz_process_oftp_resp()-488: ha nmember:1 nvcluster:0 mode:1
<16209> __is_sn_known()-356: MATCHED: idx:0 sn:FL-8HFT718900132
<16209> _faz_process_oftp_resp()-494: Received SN:FL-8HFT718900132 should update:0

<16208> _oftp_rcv()-1348: dev=global-faz type=252 pkt_len=1008
```

```
<16208> _oftp_rcv()-1348: opt=252, opt_len=996
<16208> _process_response()-960: checking opt code=252
<16208> _faz_process_oftp_resp()-488: ha nmember:1 nvcluster:0 mode:1
<16208> __is_sn_known()-356: MATCHED: idx:0 sn:FL-8HFT718900132
<16208> _faz_process_oftp_resp()-494: Received SN:FL-8HFT718900132 should update:0

<16206> _rmt_connect()-1433: oftp is ready.
<16206> _rmt_connect()-1435: xfer_status changed from 2 to 2 for global-faz
<16206> _rmt_connect()-1439: setting epoll_hd:0x141f69e0 to _rmt_rcv
<16206> _check_oftp_certificate()-248: checking sn:FL-8HFT718900132 vs cert sn:FL-
8HFT718900132
<16206> _check_oftp_certificate()-252: Verified the certificate of peer (172.18.64.234) to
match sn=FL-8HFT718900132
<16206> _faz_post_connection()-292: Certificate verification:enabled, Faz verified:1
<16206> _send_queue_item()-518: xfer_status changed from 2 to 1 for global-faz
<16206> _send_queue_item()-523: type=0, cat=0, logcount=0, len=0
<16206> _oftp_send()-487: dev=global-faz type=17 pkt_len=34

<16206> _oftp_send()-487: opt=253, opt_len=10
<16206> _oftp_send()-487: opt=81, opt_len=12
<16206> _oftp_rcv()-1348: dev=global-faz type=252 pkt_len=1008

<16206> _oftp_rcv()-1348: opt=252, opt_len=996
<16206> _process_response()-960: checking opt code=252
<16206> _faz_process_oftp_resp()-488: ha nmember:1 nvcluster:0 mode:1
<16206> __is_sn_known()-356: MATCHED: idx:0 sn:FL-8HFT718900132
<16206> _faz_process_oftp_resp()-494: Received SN:FL-8HFT718900132 should update:0

<16209> _oftp_rcv()-1348: dev=global-faz type=1 pkt_len=985

<16209> _oftp_rcv()-1348: opt=12, opt_len=16
.....
<16209> _build_ack()-784: xfer_status changed from 1 to 2 for global-faz
<16209> _process_response()-960: checking opt code=81
.....
<16209> _send_queue_item()-523: type=1, cat=0, logcount=0, len=0
<16209> _oftp_send()-487: dev=global-faz type=1 pkt_len=24

<16209> _oftp_send()-487: opt=1, opt_len=12
<16209> _send_queue_item()-523: type=7, cat=0, logcount=0, len=988
<16209> _oftp_send()-487: dev=global-faz type=252 pkt_len=1008

<16209> _oftp_send()-487: opt=252, opt_len=996
<16208> _oftp_rcv()-1348: dev=global-faz type=1 pkt_len=58

<16208> _oftp_rcv()-1348: opt=12, opt_len=16
<16208> _oftp_rcv()-1348: opt=51, opt_len=9
<16208> _oftp_rcv()-1348: opt=49, opt_len=12
<16208> _oftp_rcv()-1348: opt=52, opt_len=9
<16208> _build_ack()-784: xfer_status changed from 1 to 2 for global-faz
<16208> _process_response()-960: checking opt code=52
<16208> _send_queue_item()-523: type=1, cat=0, logcount=0, len=0
<16208> _oftp_send()-487: dev=global-faz type=1 pkt_len=24

<16208> _oftp_send()-487: opt=1, opt_len=12
```

```
<16206> _oftp_rcv()-1348: dev=global-faz type=1 pkt_len=985

.....
<16208> _send_queue_item()-523: type=3, cat=1, logcount=1, len=301
<16206> _oftp_rcv()-1348: opt=78, opt_len=55
.....
<16206> _build_ack()-784: xfer_status changed from 1 to 2 for global-faz
<16206> _process_response()-960: checking opt code=81
.....
<16206> _send_queue_item()-523: type=1, cat=0, logcount=0, len=0
<16206> _oftp_send()-487: dev=global-faz type=1 pkt_len=24

<16206> _oftp_send()-487: opt=1, opt_len=12
<16206> _send_queue_item()-523: type=7, cat=0, logcount=0, len=988
<16206> _oftp_send()-487: dev=global-faz type=252 pkt_len=1008

<16206> _oftp_send()-487: opt=252, opt_len=996
<16206> _add_change_notice_queue_item()-269: Change notice packet added to queue. len=145
.....
<16206> _send_queue_item()-523: type=2, cat=0, logcount=0, len=300
<16206> _oftp_send()-487: dev=global-faz type=37 pkt_len=300

.....

<16206> _oftp_send()-487: opt=152, opt_len=40
<16206> _oftp_send()-487: opt=74, opt_len=40
<16206> _oftp_send()-487: opt=82, opt_len=93
<16206> _oftp_rcv()-1348: dev=global-faz type=1 pkt_len=24

<16206> _oftp_rcv()-1348: opt=1, opt_len=12
<16206> _process_response()-960: checking opt code=1
```

**To check the FortiGate to FortiGate Cloud log server connection status:**

```
diagnose test application miglogd 20

FGT-B-LOG# diagnose test application miglogd 20
Home log server:
 Address: 172.16.95.92:514
Alternative log server:
 Address: 172.16.95.26:514
 oftp status: established
Debug zone info:
 Server IP: 172.16.95.92
 Server port: 514
 Server status: up
 Log quota: 102400MB
 Log used: 673MB
 Daily volume: 20480MB
 FDS arch pause: 0
 fams archive pause: 0
```

**To check real-time log statistics by log type since the miglogd daemon start:**

```
diagnose test application miglogd 4
```



```
FGT-B-LOG (global) # diagnose test application miglogd 4
info for vdom: root
disk
event: logs=1238 len=262534, Sun=246 Mon=247 Tue=197 Wed=0 Thu=55 Fri=246 Sat=247
compressed=163038
dns: logs=4 len=1734, Sun=0 Mon=0 Tue=0 Wed=0 Thu=4 Fri=0 Sat=0 compressed=453

report
event: logs=1244 len=225453, Sun=246 Mon=247 Tue=197 Wed=0 Thu=61 Fri=246 Sat=247

faz
event: logs=6 len=1548, Sun=0 Mon=0 Tue=6 Wed=0 Thu=0 Fri=0 Sat=0 compressed=5446

info for vdom: vdom1
memory
traffic: logs=462 len=389648, Sun=93 Mon=88 Tue=77 Wed=0 Thu=13 Fri=116 Sat=75
event: logs=3724 len=1170237, Sun=670 Mon=700 Tue=531 Wed=0 Thu=392 Fri=747 Sat=684
app-ctrl: logs=16 len=9613, Sun=3 Mon=3 Tue=3 Wed=0 Thu=0 Fri=5 Sat=2
dns: logs=71 len=29833, Sun=0 Mon=0 Tue=0 Wed=0 Thu=71 Fri=0 Sat=0

disk
traffic: logs=462 len=389648, Sun=93 Mon=88 Tue=77 Wed=0 Thu=13 Fri=116 Sat=75
compressed=134638
event: logs=2262 len=550957, Sun=382 Mon=412 Tue=307 Wed=0 Thu=306 Fri=459 Sat=396
compressed=244606
app-ctrl: logs=16 len=9613, Sun=3 Mon=3 Tue=3 Wed=0 Thu=0 Fri=5 Sat=2 compressed=3966
dns: logs=71 len=29833, Sun=0 Mon=0 Tue=0 Wed=0 Thu=71 Fri=0 Sat=0 compressed=1499

report
traffic: logs=462 len=375326, Sun=93 Mon=88 Tue=77 Wed=0 Thu=13 Fri=116 Sat=75
event: logs=3733 len=1057123, Sun=670 Mon=700 Tue=531 Wed=0 Thu=401 Fri=747 Sat=684
app-ctrl: logs=16 len=9117, Sun=3 Mon=3 Tue=3 Wed=0 Thu=0 Fri=5 Sat=2

faz
traffic: logs=462 len=411362, Sun=93 Mon=88 Tue=77 Wed=0 Thu=13 Fri=116 Sat=75
compressed=307610
event: logs=3733 len=1348297, Sun=670 Mon=700 Tue=531 Wed=0 Thu=401 Fri=747 Sat=684
compressed=816636
app-ctrl: logs=16 len=10365, Sun=3 Mon=3 Tue=3 Wed=0 Thu=0 Fri=5 Sat=2 compressed=8193
dns: logs=71 len=33170, Sun=0 Mon=0 Tue=0 Wed=0 Thu=71 Fri=0 Sat=0 compressed=0
```

### To check log statistics to the local/remote log device since the miglogd daemon start:

```
diagnose test application miglogd 6 1 <<< 1 means the first child daemon
diagnose test application miglogd 6 2 <<< 2 means the second child daemon

FGT-B-LOG (global) # diagnose test application miglogd 6 1
mem=4288, disk=4070, alert=0, alarm=0, sys=5513, faz=4307, webt=0, fds=0
interface-missed=208
Queues in all miglogds: cur:0 total-so-far:36974
global log dev statistics:
syslog 0: sent=6585, failed=152, relayed=0
faz 0: sent=13, failed=0, cached=0, dropped=0 , relayed=0
```

**To check the miglogd daemon number and increase/decrease miglogd daemon:**

```
diagnose test application miglogd 15 <<< Show miglog ID
diagnose test application miglogd 13 <<< Increase one miglogd child
diagnose test application miglogd 14 <<< Decrease one miglogd child

FGT-B-LOG (global) # diagnose test application miglogd 15
Main miglogd: ID=0, children=2, active-children=2
 ID=1, duration=70465.
 ID=2, duration=70465.

FGT-B-LOG (global) # diagnose test application miglogd 13

FGT-B-LOG (global) # diagnose test application miglogd 15
Main miglogd: ID=0, children=3, active-children=3
 ID=1, duration=70486.
 ID=2, duration=70486.
 ID=3, duration=1.

FGT-B-LOG (global) # diagnose test application miglogd 14

FGT-B-LOG (global) # diagnose test application miglogd 15
Main miglogd: ID=0, children=2, active-children=2
 ID=1, duration=70604.
 ID=2, duration=70604.
```

## Backing up log files or dumping log messages

When a log issue is caused by a particular log message, it is very help to get logs from that FortiGate. This topic provides steps for using `execute log backup` or dumping log messages to a USB drive.

### Backing up full logs using `execute log backup`

This command backs up all disk log files and is only available on FortiGates with an SSD disk.

Before running `execute log backup`, we recommend temporarily stopping `miglogd` and `reportd`.

**To stop and kill miglogd and reportd:**

```
diagnose sys process daemon-auto-restart disable miglogd
diagnose sys process daemon-auto-restart disable reportd
```

Or

1. Determine the process, or thread, ID (PID) of `miglogd` and `reportd`:

```
diagnose sys top 10 99
```

2. Kill each process:

```
diagnose sys kill 9 <PID>
```

**To store the log file on a USB drive:**

1. Plug in a USB drive into the FortiGate.
2. Run this command:

```
exec log backup /usb/log.tar
```

**To restart miglogd and reportd:**

```
diagnose sys process daemon-auto-restart enable miglogd
diagnose sys process daemon-auto-restart enable reportd
```

**Dumping log messages****To dump log messages:**

1. Enable log dumping for miglogd daemon:

```
(global) # diagnose test application miglogd 26 1
miglogd(1) log dumping is enabled
```

2. Display all miglogd dumping status:

```
global) # diagnose test application miglogd 26 0 255
miglogd(0) log dumping is disabled
miglogd(1) log dumping is enabled
miglogd(2) log dumping is disabled
```

```
(global) # diagnose test application miglogd 26 2
miglogd(2) log dumping is enabled
```

```
(global) # diagnose test application miglogd 26 0
miglogd(0) log dumping is enabled
```

```
(global) # diagnose test application miglogd 26 0 255
miglogd(0) log dumping is enabled
miglogd(1) log dumping is enabled
miglogd(2) log dumping is enabled
```

3. Let the FortiGate run and collect log messages.
4. List the log dump files:

```
(global) # diagnose test application miglogd 33
2019-04-17 15:50:02 20828 log-1-0.dat
2019-04-17 15:48:31 4892 log-2-0.dat
```

5. Back up log dump files to the USB drive:

```
(global) # diagnose test application miglogd 34
```

```
Dumping file miglog1_index0.dat copied to USB disk OK.
```

```
Dumping file miglog2_index0.dat copied to USB disk OK.
```

6. Disable log dumping for miglogd daemon:

```
(global) # diagnose test application miglogd 26 0
miglogd(0) log dumping is disabled
```

```
(global) # diagnose test application miglogd 26 1
miglogd(1) log dumping is disabled

(global) # diagnose test application miglogd 26 2
miglogd(2) log dumping is disabled

(global) # diagnose test application miglogd 26 0 255
miglogd(0) log dumping is disabled
miglogd(1) log dumping is disabled
miglogd(2) log dumping is disabled
```

## SNMP OID for logs that failed to send

When a syslog server encounters low-performance conditions and slows down to respond, the buffered syslog messages in the kernel might overflow after a certain number of retransmissions, causing the overflowed messages to be lost. OIDs track the lost messages or failed logs.

SNMP query OIDs include log statistics for global log devices:

- FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgLog.fgLogDeviceNumber 1.3.6.1.4.1.12356.101.21.1.1
- FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgLog.fgLogDevices.fgLogDeviceTable.fgLogDeviceEntry.fgLogDeviceEntryIndex 1.3.6.1.4.1.12356.101.21.2.1.1.1
- FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgLog.fgLogDevices.fgLogDeviceTable.fgLogDeviceEntry.fgLogDeviceEnabled 1.3.6.1.4.1.12356.101.21.2.1.1.2
- FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgLog.fgLogDevices.fgLogDeviceTable.fgLogDeviceEntry.fgLogDeviceName 1.3.6.1.4.1.12356.101.21.2.1.1.3
- FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgLog.fgLogDevices.fgLogDeviceTable.fgLogDeviceEntry.fgLogDeviceSentCount 1.3.6.1.4.1.12356.101.21.2.1.1.4
- FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgLog.fgLogDevices.fgLogDeviceTable.fgLogDeviceEntry.fgLogDeviceRelayedCount 1.3.6.1.4.1.12356.101.21.2.1.1.5
- FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgLog.fgLogDevices.fgLogDeviceTable.fgLogDeviceEntry.fgLogDeviceCachedCount 1.3.6.1.4.1.12356.101.21.2.1.1.6
- FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgLog.fgLogDevices.fgLogDeviceTable.fgLogDeviceEntry.fgLogDeviceFailedCount 1.3.6.1.4.1.12356.101.21.2.1.1.7
- FORTINET-FORTIGATE-MIB:fortinet.fnFortiGateMib.fgLog.fgLogDevices.fgLogDeviceTable.fgLogDeviceEntry.fgLogDeviceDroppedCount 1.3.6.1.4.1.12356.101.21.2.1.1.8

Where:

- fgLogDeviceNumber is the number of devices in the table.
- fgLogDeviceEnabled is either 1 or 0, indicating whether the device is enabled.
- fgLogDeviceName is the name of the device.

A FortiGate connected to a syslog server or FortiAnalyzer generates statistics that can be seen using the `diagnose test application miglogd` command:

```
(global) # diagnose test application miglogd 6
mem=404, disk=657, alert=0, alarm=0, sys=920, faz=555, webt=0, fds=0
interface-missed=460
Queues in all miglogds: cur:0 total-so-far:526
global log dev statistics:
syslog 0: sent=254, failed=139, relayed=0
syslog 1: sent=220, failed=139, relayed=0
syslog 2: sent=95, failed=73, relayed=0
faz 0: sent=282, failed=0, cached=0, dropped=0 , relayed=0
Num of REST URLs: 3
/api/v2/monitor/system/csf/ : 0 : 300
/api/v2/cmdb/system/interface/ : 394.0.673.15877729363538323653.1547149763 : 1200
/api/v2/monitor/system/ha-checksums/ : 0 : 1200
faz 1: sent=272, failed=0, cached=0, dropped=0 , relayed=0
Num of REST URLs: 2
/api/v2/monitor/system/csf/ : 0 : 300
/api/v2/cmdb/system/interface/ : 394.0.673.15877729363538323653.1547149763 : 1200
```

The same statistics are also available in snmpwalk/snmpget on the OID 1.3.6.1.4.1.12356.101.21.

```
snmpwalk -v2c -c REGR-SYS 172.16.200.1 1.3.6.1.4.1.12356.101.21
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.1.1.0 = INTEGER: 9
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.1.0 = INTEGER: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.1.1 = INTEGER: 1
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.1.2 = INTEGER: 2
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.1.3 = INTEGER: 3
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.1.4 = INTEGER: 4
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.1.5 = INTEGER: 5
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.1.6 = INTEGER: 6
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.1.7 = INTEGER: 7
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.1.8 = INTEGER: 8
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.2.0 = INTEGER: 1
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.2.1 = INTEGER: 1
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.2.2 = INTEGER: 1
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.2.3 = INTEGER: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.2.4 = INTEGER: 1
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.2.5 = INTEGER: 1
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.2.6 = INTEGER: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.2.7 = INTEGER: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.2.8 = INTEGER: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.3.0 = STRING: "syslog"
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.3.1 = STRING: "syslog2"
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.3.2 = STRING: "syslog3"
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.3.3 = STRING: "syslog4"
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.3.4 = STRING: "faz"
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.3.5 = STRING: "faz2"
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.3.6 = STRING: "faz3"
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.3.7 = STRING: "webtrends"
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.3.8 = STRING: "fds"
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.4.0 = Counter32: 254
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.4.1 = Counter32: 220
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.4.2 = Counter32: 95
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.4.3 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.4.4 = Counter32: 282
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.4.5 = Counter32: 272
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.4.6 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.4.7 = Counter32: 0
```

```
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.4.8 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.5.0 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.5.1 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.5.2 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.5.3 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.5.4 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.5.5 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.5.6 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.5.7 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.5.8 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.6.0 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.6.1 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.6.2 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.6.3 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.6.4 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.6.5 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.6.6 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.6.7 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.6.8 = Gauge32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.7.0 = Counter32: 139
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.7.1 = Counter32: 139
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.7.2 = Counter32: 73
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.7.3 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.7.4 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.7.5 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.7.6 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.7.7 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.7.8 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.8.0 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.8.1 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.8.2 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.8.3 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.8.4 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.8.5 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.8.6 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.8.7 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.8.8 = Counter32: 0
```

### To get the type of logging device that is attached to the FortiGate:

```
root@PC05:/home/tester/autolib/trunk# snmpwalk -v2c -c REGR-SYS 172.16.200.1
1.3.6.1.4.1.12356.101.21.2.1.1.3
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.3.0 = STRING: "syslog"
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.3.1 = STRING: "syslog2"
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.3.2 = STRING: "syslog3"
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.3.3 = STRING: "syslog4"
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.3.4 = STRING: "faz"
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.3.5 = STRING: "faz2"
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.3.6 = STRING: "faz3"
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.3.7 = STRING: "webtrends"
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.3.8 = STRING: "fds"
```

### To get the present state of the logging device that is attached to the FortiGate:

```
root@PC05:/home/tester/autolib/trunk# snmpwalk -v2c -c REGR-SYS 172.16.200.1
1.3.6.1.4.1.12356.101.21.2.1.1.2
```

```
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.2.0 = INTEGER: 1
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.2.1 = INTEGER: 1
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.2.2 = INTEGER: 1
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.2.3 = INTEGER: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.2.4 = INTEGER: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.2.5 = INTEGER: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.2.6 = INTEGER: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.2.7 = INTEGER: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.2.8 = INTEGER: 0
```

### To get the failed log count value:

```
root@PC05:/home/tester/autolib/trunk# snmpwalk -v2c -c REGR-SYS 172.16.200.1
1.3.6.1.4.1.12356.101.21.2.1.1.7
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.7.0 = Counter32: 139
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.7.1 = Counter32: 139
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.7.2 = Counter32: 73
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.7.3 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.7.4 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.7.5 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.7.6 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.7.7 = Counter32: 0
FORTINET-FORTIGATE-MIB::fnFortiGateMib.21.2.1.1.7.8 = Counter32: 0
```

# Monitor

The following sections provide information about monitoring:

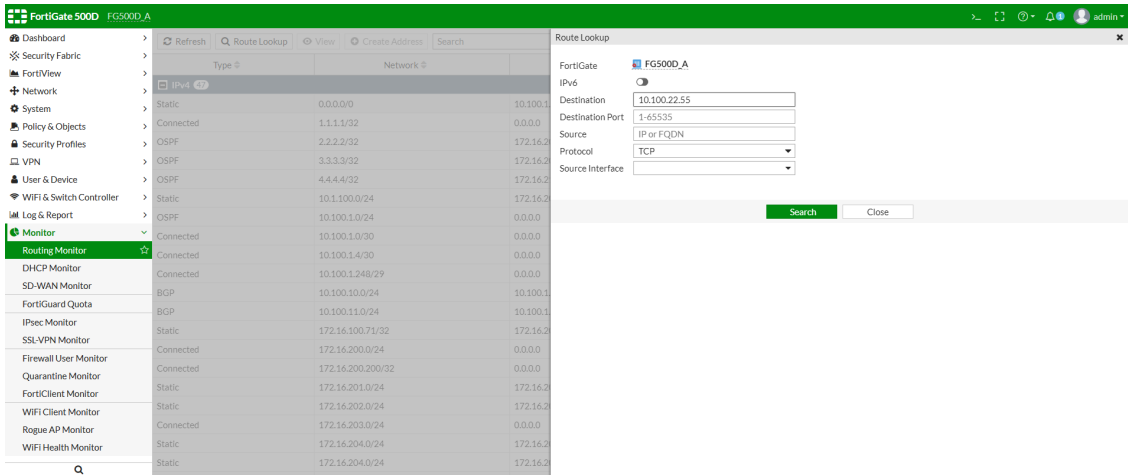
- [Policy and route checks on page 1658](#)
- [WiFi client monitor on page 1660](#)
- [WiFi health monitor on page 1661](#)
- [Running processes on page 1662](#)
- [Aggregate processes information on page 1664](#)

## Policy and route checks

Policy route look up is prioritized over static and dynamic routes when doing a route look up in the GUI.

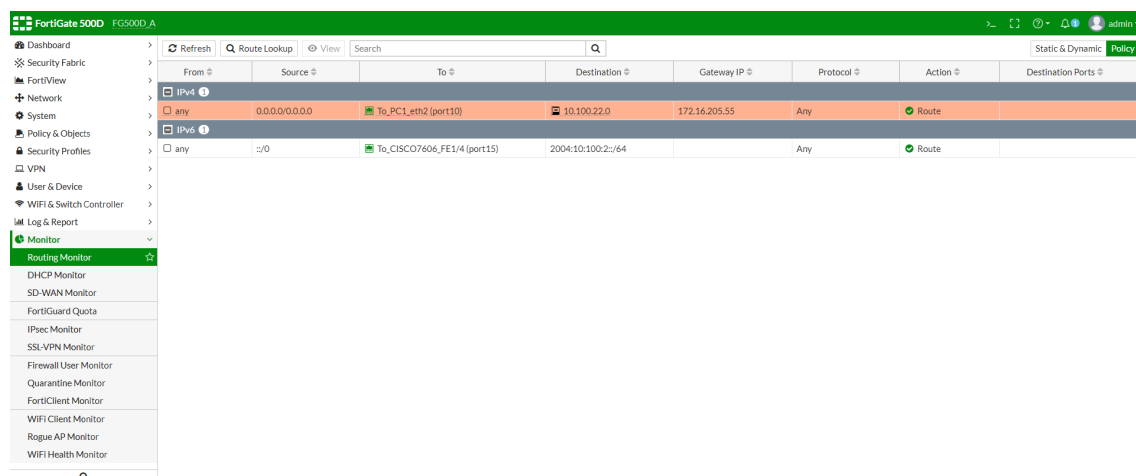
To look up an IPv4 route in the GUI:

1. Go to *Monitor > Routing Monitor*.
2. Click *Route Lookup*.



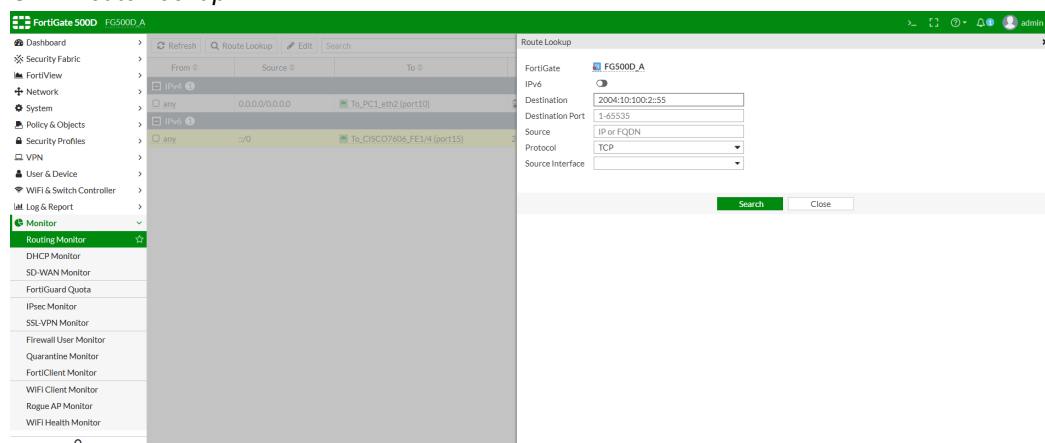
3. Enter an IP address in the *Destination* field, then click *Search*.  
The matching IPv4 route is highlighted on the *Route Monitor* page.



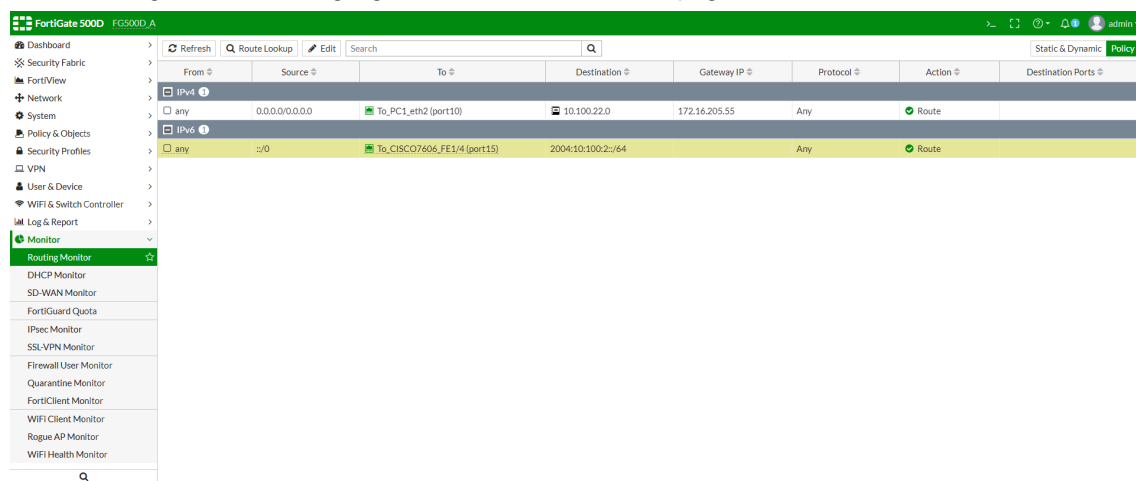


To look up an IPv6 route in the GUI:

1. Go to *Monitor > Routing Monitor*.
2. Click *Route Lookup*.



3. Enter an IPv6 address in the *Destination* field, then click *Search*.  
The matching IPv6 route is highlighted on the *Route Monitor* page.



**To look up an IPv4 route in the CLI:**

```
diagnose ip proute match <destination_ip_address> <source_ip_address> <interface_name>
<protocol> <destination_port>
```

For example:

```
diagnose ip proute match 10.100.21.44 2.2.2.2 port2 6 2
dst=10.100.21.44 src=2.2.2.2 iif=24 protocol=6 dport=2
id=7f00000c type=VWL
seq-num=12
```

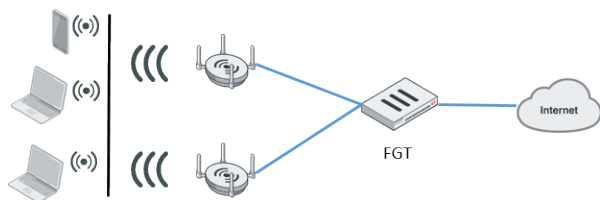
```
diagnose ip proute match 10.100.20.44 2.2.2.2 port2 6 2
dst=10.100.20.44 src=2.2.2.2 iif=24 protocol=6 dport=2
id=00000016 type=Policy Route
seq-num=22
```

**To look up an IPv6 route in the CLI:**

```
diagnose ipv6 proute match <destination_ipv6_address> <source_ipv6_address> <interface_name>
<protocol> <destination_port>
```

## WiFi client monitor

The following shows a simple network topology when using FortiAPs with FortiGate:



To view connected WiFi clients on the FortiGate unit, go to *Monitor > WiFi Client Monitor*. The following columns display:

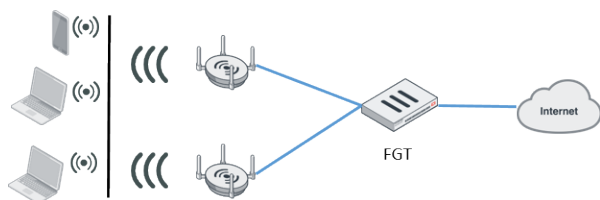
Column	Description
SSID	SSID that the client connected to, such as the tunnel, bridge, or mesh.
FortiAP	Serial number of the FortiAP unit that the client connected to.
User	Username if using WPA enterprise authentication.
IP	IP address assigned to the wireless client.
Device	Wireless client device type.
Channel	FortiAP operation channel.
Auth	Authentication type used.
Channel	WiFi radio channel in use.
Bandwidth Tx/Rx	Client received and transmitted bandwidth in Kbps.

Column	Description
Signal Strength/Noise	Signal-to-noise ratio in decibels calculated from signal strength and noise level.
Association Time	How long the client has been connected to this AP.
Device OS	Wireless device OS.
Manufacturer	Wireless device manufacturer.
MIMO	Wireless device MIMO information.

SSID	FortiAP	User	IP	Device	Channel	Bandwidth Tx/Rx	Signal Strength/Noise	Association Time	Device OS	Manufacturer	MIMO
80e_ssid_user	FP224E4T17000003	test	10.80.12.2	test-wifi	1	0 bps	66dB	2019/01/23 16:22:17	Linux / Debian	TP-LINK	1x1
80e_br1	FP224E4T17000003		10.80.0.204	Bruce_test_Dell	1	352 bps I	54dB	2019/01/23 16:33:37	Windows	Intel Corporate	1x1
80e_ssid3	FP320C3X17001889		10.80.3.2	HUAWEI_P20_Pro-89b7b01761	100	794 bps I	56dB	2019/01/23 17:05:20	Android		2x2
80e_ssid1	PS423E3X16000030		10.80.1.2	VAN-200558-NB	132	37.79 kbps	52dB	2019/01/23 17:03:58	Windows 10 / 2016	Microsoft	2x2
80e_mesh	FP224E4T17000003		10.80.0.201	90:6c:ac:8a:66:27	1	50.96 kbps	79dB	2019/01/23 16:19:24		Fortinet, Inc.	4x4

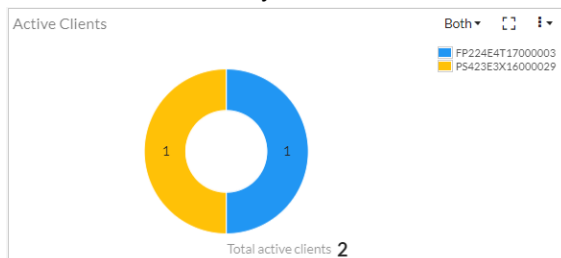
## WiFi health monitor

The following shows a simple network topology when using FortiAPs with FortiGate:

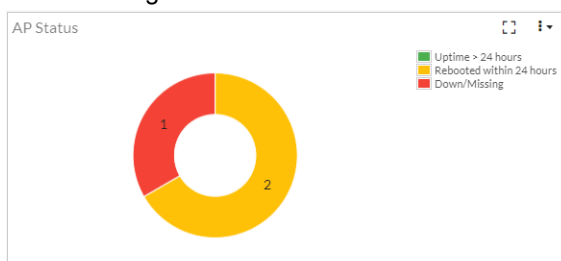


The **Monitor > WiFi Health Monitor** page displays the following charts:

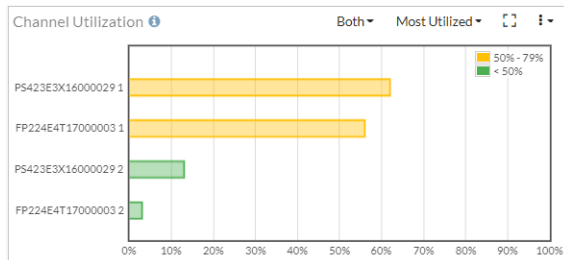
- Active Clients:** Currently active clients on each FortiAP



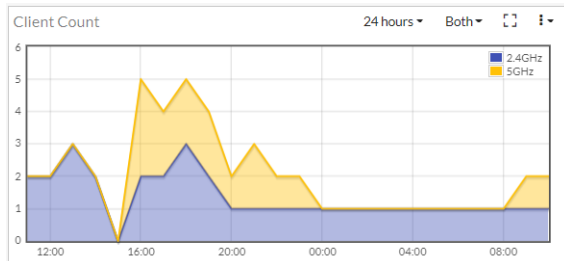
- AP Status:** APs by status, sorted by those that have been up for over 24 hours, rebooted in the past 24 hours, and down/missing



- **Channel Utilization:** Allow users to view 10-20 most and least utilized channels for each AP radio and a third histogram view showing utilization counts



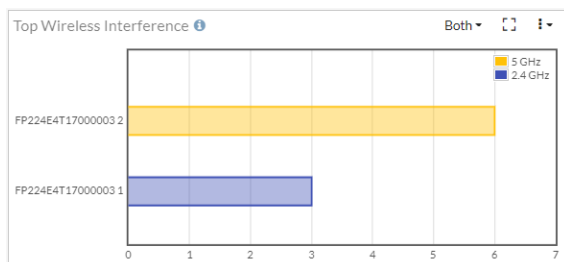
- **Client Count:** Shows client count over time. Can view for the past hour, day, or 30 days.



- **Login Failures:** Time, SSID, hostname, and username for failed login attempts. The widget also displays the AP name and group of FortiAP units with failed login attempts.

Time (UTC)	SSID	Host Name/MAC	User	AP Name	AP Group
2019/01/16 10:14:14	80e_ssld_us...	b8:81:98:bf...	usre	FP224E...	
2019/01/16 10:07:21	80e_ssld_ra...	50:1a:c5:e9...	test2	PS423E...	

- **Top Wireless Interference:** Separate widgets for 2.4 GHz and 5 GHz bands. This requires spectrum analysis to be enabled on the radios.



## Running processes

The `diagnose sys top` CLI command displays a list of processes that are running on the FortiGate device, as well as information about each process.

The following commands can be used while the command is running:

q	Quit, and return to the command prompt.
c	Sort the process list by the amount of CPU that each process is using.
m	Sort the process list by the amount of memory that each process is using.

The `get system performance top` command also performs the same function.

## Syntax

```
diagnose sys top [<delay>] [<lines>]
```

Variable	Description
<delay>	The delay between updates of the process list, in seconds (default = 5).
<lines>	The maximum number of processes that are displayed in the output (default = 20).

## Example output

```
diagnose sys top 5 5
Run Time: 4 days, 5 hours and 29 minutes
1U, 0N, 0S, 99I, 0WA, 0HI, 0SI, 0ST; 1866T, 1113F
 miglogd 191 S 0.3 6.3
 newcli 18391 R 0.1 0.3
 cmdbsvr 99 S 0.3 1.4
 pyfcgid 15628 S 0.0 1.3
 ipshelper 164 S < 0.3 1.2
```

Keyword / Variable / Column	Description
Run Time	How long the FortiOS has been running, as a string.
U	The percentage of user space applications using the CPU. In the example, 1U means that 1% of user space applications are using the CPU.
N	Nice, or higher priority, processes, as a percentage.
S	System, or kernel, processes that are using the CPU, as a percentage.
I	The idle CPU usage, as a percentage.
WA	The IO wait, as a percentage.
HI	The hardware interrupts, as a percentage of CPU time used.
SI	The software interrupts, as a percentage of CPU time used.
ST	The steal time, as a percentage.
T	The total FortiOS system memory, in MB. In the example, 1866T means that there is 1866 MB of system memory.
F	The total free memory, in MB. In the example 1113F means that there are 1113 MB of free memory.

Keyword / Variable / Column	Description
Column 1	The process name, such as <code>mglogd</code> , or <code>newcli</code> .
Column 2	The process ID number (PID).
Column 3	The process status: <ul style="list-style-type: none"> <li>R: running</li> <li>S: sleeping</li> <li>Z: zombie</li> <li>D: disk sleep</li> </ul> A < on a process means that it is high priority.
Column 4	The CPU usage.
Column 5	The memory usage.

## Stop a running process

The `diagnose sys kill` command can be used to stop a running process.

### Syntax

```
diagnose sys kill <signal> <PID>
```

Variable	Description
<signal>	<p>A number between 1 and 32.</p> <p>Each number represents a signal sent to kill the process. Signal 11 is commonly used to send the SIGSEGV signal, causing the process to generate a Segmentation Fault crashlog. Signal 9, SIGKILL, forces the process to terminate immediate.</p> <p>For more information about kill commands and signals, see <a href="https://www.linux.org/threads/kill-commands-and-signals.8881">https://www.linux.org/threads/kill-commands-and-signals.8881</a>.</p>
<PID>	The process ID of the process to be killed.

### Example

To kill the `newcli` process from the previous example and generate a Segmentation Fault crashlog, enter the following:

```
diagnose sys kill 11 18391
```

## Aggregate processes information

The `diagnose sys top-summary` CLI command shows the top aggregate processes information.

The following commands can be used while the command is running:

h or ?	Show the list of available commands
q or <Ctrl> C	Quit, and return to the command prompt.
m	Sort by memory consumption.
c	Sort by CPU percentage.
f	Sort by the number of open file descriptors.
p	Sort by PID.
k or <Up>	Go up in the list of processes.
j or <Down>	Go down in the list of processes.
<Enter> or <Space>	Toggle the process tree.

## Syntax

```
diagnose sys top-summary <options>
```

Options	Description
-n LINES or --num=LINES	The number of top processes to show (default = 20).
-i INTERVAL or --interval=INTERVAL	The update interval, in seconds (default = 1).
-s SORT or --sort=sort	The sort mode: <ul style="list-style-type: none"> <li>• cpu_percent: Sort by CPU percentage (default).</li> <li>• mem: Sort by memory consumption,</li> <li>• fds: Sort by the number of open file descriptors.</li> <li>• pid: Sort by PID.</li> </ul>
-h or --help	Show the help message and exit.

## Example output

```
diagnose sys top-summary '-n 5 --sort=mem'
CPU [|] 4.8%
Mem [||||||||||||||||] 54.0% 1100M/2012M
Processes: 5 (running=1 sleeping=106)
PID RSS CPU% ^MEM% FDS TIME+ NAME
* 150 67M 0.0 3.4 22 01:11.84 httpsd [x4]
 171 57M 0.0 2.8 100 00:21.99 wad [x6]
 8050 46M 0.0 2.3 12 00:00.38 pyfcgid [x4]
 168 45M 0.0 2.3 16 00:05.57 reportd
 159 41M 0.0 2.1 26 00:48.88 forticron
```

The output shows five lines, sorted in descending order by memory consumption.

- ^ indicates the parameter that the information is sorted by.
- \* indicates the currently active line.

Press **c** to sort the processes by CPU utilization, then press **<Down>** four times to select the miglogd parent instance, and then press **<Enter>** to see details about the child instance:

```
CPU [|] 4.8%
Mem [||||||||||||||||] 54.0% 1099M/2012M
Processes: 5 (running=1 sleeping=106)
PID RSS ^CPU% MEM% FDS TIME+ NAME
180 35M 4.8 1.8 12 00:01.51 sshd [x4]
134 9M 0.0 0.5 88 00:09.99 zebos_launcher [x12]
135 6M 0.0 0.3 12 00:01.45 bfdd
147 6M 0.0 0.3 12 00:00.70 uploadd
* 148 22M 0.0 1.1 103 01:29.71 miglogd [x2]
 203 22M 0.0 1.1 42 00:44.53 miglogd
```



# VM

## Amazon Web Services

See the *FortiOS 6.2 AWS Administration Guide*.

## Microsoft Azure

See the *FortiOS 6.2 Azure Administration Guide*.

## Google Cloud Platform

See the *FortiOS 6.2 GCP Administration Guide*.

## Oracle OCI

See the *FortiOS 6.2 OCI Administration Guide*.

## AliCloud

See the *FortiOS 6.2 AliCloud Administration Guide*.

## Private cloud

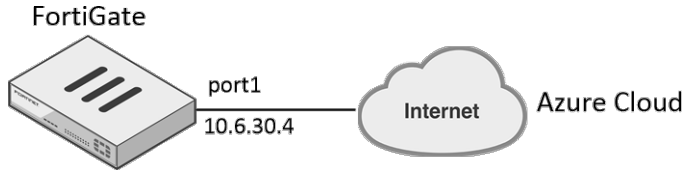
See the *FortiOS 6.2 VMware ESXi Administration Guide*.

## FortiGate multiple connector support

This guide shows how to configure Fabric connectors and resolve dynamic firewall addresses through the configured Fabric connector in FortiOS.

FortiOS supports multiple Fabric connectors including public connectors (AWS, Azure, GCP, OCI, AliCloud) and private connectors (Kubernetes, VMware ESXi, VMware NSX, OpenStack, Cisco ACI, Nuage). FortiOS also supports multiple instances for each type of Fabric connector.

This guide uses an Azure Fabric connector as an example. The configuration procedure for all supported Fabric connectors is the same. In the following topology, the FortiGate accesses the Azure public cloud through the Internet:



This process consists of the following:

1. [Configure the interface.](#)
2. [Configure a static route to connect to the Internet.](#)
3. [Configure two Azure Fabric connectors with different client IDs.](#)
4. [Check the configured Fabric connectors.](#)
5. [Create two firewall addresses.](#)
6. [Check the resolved firewall addresses after the update interval.](#)
7. [Run diagnose commands.](#)

#### To configure the interface:

1. In FortiOS, go to *Network > Interfaces*.
2. Edit port1:
  - a. From the *Role* dropdown list, select *WAN*.
  - b. In the *IP/Network Mask* field, enter 10.6.30.4/255.255.255.0 for the interface connected to the Internet.

#### To configure a static route to connect to the Internet:

1. Go to *Network > Static Routes*. Click *Create New*.
2. In the *Destination* field, enter 0.0.0.0/0.0.0.0.
3. From the *Interface* dropdown list, select *port1*.
4. In the *Gateway Address* field, enter 10.60.30.254.

#### To configure two Azure Fabric connectors with different client IDs:

1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New*. Configure the first Fabric connector:
  - a. Select *Microsoft Azure*.
  - b. In the *Name* field, enter azure1.
  - c. In the *Status* field, select *Enabled*.
  - d. From the *Server region* dropdown list, select *Global*.
  - e. In the *Tenant ID* field, enter the tenant ID. In this example, it is 942b80cd-1b14-42a1-8dcf-4b21dece61ba.
  - f. In the *Client ID* field, enter the client ID. In this example, it is 14dbd5c5-307e-4ea4-8133-68738141feb1.
  - g. In the *Client secret* field, enter the client secret.
  - h. Leave the *Resource path* disabled.
  - i. Click *OK*.

3. Click *Create New*. Configure the second Fabric connector:
  - a. Select *Microsoft Azure*.
  - b. In the *Name* field, enter *azure2*.
  - c. In the *Status* field, select *Enabled*.
  - d. From the *Server* region dropdown list, select *Global*.
  - e. In the *Tenant ID* field, enter the tenant ID. In this example, it is 942b80cd-1b14-42a1-8dcf-4b21dece61ba.
  - f. In the *Client ID* field, enter the client ID. In this example, it is 3baf0a6c-44ff-4f94-b292-07f7a2c36be6.
  - g. In the *Client secret* field, enter the client secret.
  - h. Leave the *Resource path* disabled.
  - i. Click *OK*.

#### To check the configured Fabric connectors:

1. Go to *Security Fabric > Fabric Connectors*.
2. Click the *Refresh* icon in the upper right corner of each configured Fabric connector. A green up arrow appears in the lower right corner, meaning that both Fabric connectors are connected to the Azure cloud using different client IDs.

#### To create two firewall addresses:

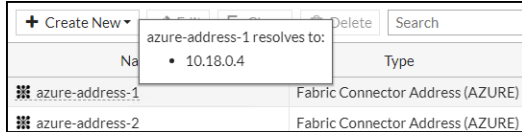
This process creates two Fabric connector firewall addresses to associate with the configured Fabric connectors.

1. Go to *Policy & Objects > Addresses*.
2. Click *Create New > Address*. Configure the first Fabric connector firewall address:
  - a. In the *Name* field, enter *azure-address-1*.
  - b. From the *Type* dropdown list, select *Fabric Connector address*.
  - c. From the *SDN Connector* dropdown list, select *azure1*.
  - d. For *SDN address type*, select *Private*.
  - e. From the *Filter* dropdown list, select the desired filter.
  - f. For *Interface*, select *any*.
  - g. Click *OK*.
3. Click *Create New > Address*. Configure the second Fabric connector firewall address:
  - a. In the *Name* field, enter *azure-address-1*.
  - b. From the *Type* dropdown list, select *Fabric Connector address*.
  - c. From the *SDN Connector* dropdown list, select *azure2*.
  - d. For *SDN address type*, select *Private*.
  - e. From the *Filter* dropdown list, select the desired filter.
  - f. For *Interface*, select *any*.
  - g. Click *OK*.

#### To check the resolved firewall addresses after the update interval:

By default, the update interval is 60 seconds.

1. Go to *Policy & Objects > Addresses*.
2. Hover over the created addresses. The firewall address that the configured Fabric connectors resolved display.



### To run diagnose commands:

Run the `show sdn connector status` command. Both Fabric connectors should appear with a status of connected.

Run the `diagnose debug application azd -1` command. The output should look like the following:

```
Level2-downstream-D # diagnose debug application azd -1
...
azd sdn connector azure1 start updating IP addresses
azd checking firewall address object azure-address-1, vd 0
IP address change, new list:
10.18.0.4
...
```

To restart the Azure Fabric connector daemon, run the `diagnose test application azd 99` command.

## Adding VDOMs with FortiGate v-series

Each FortiGate-VM base license type allows a default number of VDOMs. This recipe provides sample procedures to add VDOMs beyond the default number using separately purchased VDOM licenses.

This recipe consists of the following steps:

1. [Activate the FortiGate-VM with the base license.](#)
2. [Add more VDOMs to the FortiGate-VM.](#)

### To activate the FortiGate-VM with the base license:

1. Purchase and register the FortiGate-VM base license in FortiCare:
  - a. Purchase the FortiGate-VM base license from Fortinet or a Fortinet reseller.
  - b. You receive a license certification with a registration code. Open the certification.
  - c. Log in to [Fortinet Customer Service & Support](#).
  - d. Go to *Asset > Register/Activate* and enter the provided registration code.
  - e. Follow the registration process. The serial number generates and displays on the *Registration Completion* page.
  - f. Go to *Asset > Manage/View Products*. Click the serial number to download the license file.
2. Upload the FortiGate-VM base license file to FortiOS:
  - a. Log in to the FortiGate-VM GUI.
  - b. In *Dashboard > Status*, in the *Virtual Machine* widget, click *FortiGate VM License*.
  - c. Click the *Upload* button.
  - d. Select the FortiGate-VM base license file, then click *OK*. The FortiGate-VM reboots after applying the base license.

### 3. Verify the FortiGate-VM base license status and VDOM information:

- a. Log in to the FortiGate-VM GUI.
- b. In *Dashboard > Status*, in the *Virtual Machine* widget, ensure that there is a checkmark in front of the FortiGate-VM base license name. The checkmark indicates that the base license is valid.
- c. You can check VDOM information using the CLI. The following output shows that the maximum number of VDOMs is currently one. This is correct since the FortiGate-VM base license only supports the default root VDOM that the system uses.

```
FGVM4VTM19000476 # get system status
Version: FortiGate-VM64 v6.2.0,build0866,190328 (GA)
Virus-DB: 69.00091(2019-06-07 12:19)
Extended DB: 1.00000(2018-04-09 18:07)
Extreme DB: 1.00000(2018-04-09 18:07)
IPS-DB: 14.00610(2019-05-09 00:14)
IPS-ETDB: 0.00000(2001-01-01 00:00)
APP-DB: 14.00610(2019-05-09 00:14)
INDUSTRIAL-DB: 14.00610(2019-05-09 00:14)
Serial-Number: FGVM4VTM19000476
IPS Malicious URL Database: 2.00325(2019-06-07 03:56)
Botnet DB: 4.00490(2019-05-30 10:00)
License Status: Valid
License Expires: 2020-04-30
VM Resources: 2 CPU/4 allowed, 3022 MB RAM/6144 MB allowed
Log hard disk: Available
Hostname: FGVM4VTM19000476
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 1
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 0866
Release Version Information: GA
FortiOS x86-64: Yes
System time: Fri Jun 7 14:04:55 2019
```

### To add more VDOMs to the FortiGate-VM:

You can repeat this procedure multiple times to stack multiple VDOM licenses on the same FortiGate-VM.

1. Purchase and register the FortiGate-VM upgrade license in FortiCare. This example adds 15 VDOMs:
  - a. Purchase the FortiGate-VM upgrade license from Fortinet or a Fortinet reseller.
  - b. You receive a license certification with a registration code. Open the certification.
  - c. Log in to [Fortinet Customer Service & Support](#).
  - d. Go to *Asset > Register/Activate* and enter the provided registration code.
  - e. On the *Specify License Confirmation Information* screen, enter the FortiGate-VM serial number to apply the VDOM upgrade license to the FortiGate-VM. In this example, the FortiGate-VM serial number is *FGVM4VTM19000476*.

Customer Service & Support Home **Asset** Assistance Download Feedback 196068 fortinet

License Registration

Registration Code: HK48V-5C01C-G6BRE-GT6VN-ECW1AD

1 Registration Code > 2 **Registration Info** > 3 Completion

Specify License Confirmation Information

FortiOS 5.4 and above is required for this VDOM license to work correctly. If your unit is running FortiOS before 5.4, the actual number of VDOMs may be less.  
Enter your serial number below to register VDOM Upgrade license

The Product Serial Number is:

f. Follow the registration process.

g. Go to **Asset > Manage/View Products >** . Select the desired product, then click **License & Key**. The VDOM upgrade license displays under **Registered License(s)**, and a key for adding 15 VDOMs (in this example **M6JSD-8EE32-VHIJB-N**) displays under **Available Key(s)**.

Customer Service & Support Home **Asset** Assistance Download Feedback 196068 fortinet

Product Details FortiGate VM04V  
FGVM4VTM19000476

Back To List

Information

- General
- Location
- Entitlement
- License & Key**
- Statistics

Registration

- Renew Contract
- Add Licenses

Assistance

- Ticket List
- Technical Request
- Customer Service

Registered License(s)

License Type	License Number	Registration Date
VDOM Upgrade	VDOM4713241427	2018-04-13
Virtual Domain License Add 15		
FortiGateVM	FGVM4713410408	2019-04-29
FortiGate-VM for all supported platforms. 4 x vCPU core and up to 6GB RAM		

Available Key(s)

Key	License Number	Description
<a href="#">Get The License File</a>	FGVM4713410408	FortiGate-VM for all supported platforms. 4 x vCPU core and up to 6GB RAM
M6JSD-8EE32-VHIJB-N	VDOM4713241427	Virtual Domain License for 15

Firmware & General Updates Will Expire On 2020-04-29

2. Apply the FortiGate-VM upgrade license key to FortiOS:

a. Log in to the FortiGate-VM CLI in the local console or using SSH.

b. Apply the VDOM upgrade license key:

```
FGVM4VTM19000476 # execute upd-vd-license M6JSD-8EE32-VHIJB-N
update vdom license succeeded
```

3. Verify the FortiGate-VM VDOM information:

a. Log in to the FortiGate-VM CLI in the local console or using SSH.

b. Check VDOM information using the CLI. The following output shows that the maximum number of VDOMs is currently 15. When you add VDOMs for the first time on a FortiGate-VM v-series instance, FortiOS does not count the default VDOM, as the default VDOM is the so-called root VDOM that the system uses and FortiOS does not treat it as a countable VDOM in terms of VDOM addition. Therefore, as in this example, if your FortiGate-VM had the default VDOM configuration, then you add 15 VDOMs, FortiOS displays the maximum VDOM number as 15, not 16.

```
FGVM4VTM19000476 # get system status
Version: FortiGate-VM64 v6.2.0,build0866,190328 (GA)
Virus-DB: 69.00091(2019-06-07 12:19)
Extended DB: 1.00000(2018-04-09 18:07)
Extreme DB: 1.00000(2018-04-09 18:07)
IPS-DB: 14.00610(2019-05-09 00:14)
IPS-ETDB: 0.00000(2001-01-01 00:00)
APP-DB: 14.00610(2019-05-09 00:14)
INDUSTRIAL-DB: 14.00610(2019-05-09 00:14)
Serial-Number: FGVM4VTM19000476
IPS Malicious URL Database: 2.00325(2019-06-07 03:56)
```

```
Botnet DB: 4.00490(2019-05-30 10:00)
License Status: Valid
License Expires: 2020-04-30
VM Resources: 2 CPU/4 allowed, 3022 MB RAM/6144 MB allowed
Log hard disk: Available
Hostname: FGVM4VTM19000476
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 15
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 0866
Release Version Information: GA
FortiOS x86-64: Yes
System time: Fri Jun 7 14:39:27 2019
```

## Terraform: FortiOS as a provider

Fortinet's Terraform support provides customers with more ways to efficiently deploy, manage, and automate security across physical FortiGate appliances and virtual environments. You can use Terraform to automate various IT infrastructure needs, thereby diminishing mistakes from repetitive manual configurations.

For example, if Fortinet is releasing a new FortiOS version, your organization may require you to test a new functionality to determine how it may impact the environment before globally deploying the new version. In this case, the ability to rapidly stand up environments and test these functions prior to production environment integration provides a resource-efficient and fault-tolerant approach.

The following example demonstrates how to use the Terraform FortiOS provider to perform simple configuration changes on a FortiGate unit. It requires the following:

- FortiOS 6.0 or later
- [FortiOS Provider](#): This example uses terraform-provider-fortios 1.0.0.
- [Terraform](#): This example uses Terraform 0.11.14.
- REST API administrator created on the FortiGate with the API key

For more information, see the Terraform FortiOS Provider at <https://www.terraform.io/docs/providers/fortios/index.html>.

### To create a REST API administrator:

1. On the FortiGate, go to *System > Administrators* and click *Create New > REST API Admin*.
2. Enter the *Username* and, optionally, enter *Comments*.
3. Select an *Administrator Profile*.
4. We recommend that you create a new profile with minimal privileges for this terraform script:
  - a. In the *Administrator Profile* drop down click *Create New*.
  - b. Enter a name for the profile.
  - c. Configure the *Access Permissions*:
    - *None*: The REST API is not permitted access to the resource.
    - *Read*: The REST API can send read requests (`HTTP GET`) to the resource.

- **Read/Write:** The REST API can send read and write requests (HTTP GET/POST/PUT/DELETE) to the resource.

d. Click OK.

5. Enter *Trusted Hosts* to specify the devices that are allowed to access this FortiGate.

6. Click OK.

An API key is displayed. This key is only shown once, so you must copy and store it securely.

### To configure FortiGate with Terraform Provider module support:

1. Download the terraform-provider-fortios file to a directory on the management computer.

2. Create a new file with the .tf extension for configuring your FortiGate:

```
root@mail:/home/terraform# ls
terraform-provider-fortios_v1.0.0_x4 test.tf
```

3. Edit the test.tf Terraform configuration file:

In this example, the FortiGate's IP address is 10.6.30.5, and the API user token is 17b\*\*\*\*\*63ck. Your provider information must also be changed.

```
Configure the FortiOS Provider
provider "fortios" {
 hostname = "10.6.30.5"
 token = "17b*****63ck"
}
```

4. Create the resources for configuring your DNS object and adding a static route:

```
resource "fortios_system_setting_dns" "test1" {
 primary = "172.16.95.16"
 secondary = "8.8.8.8"
}

resource "fortios_networking_route_static" "test1" {
 dst = "110.2.2.122/32"
 gateway = "2.2.2.2"
 blackhole = "disable"
 distance = "22"
 weight = "3"
 priority = "3"
 device = "port2"
 comment = "Terraform test"
}
```

5. Save your Terraform configuration file.

6. In the terminal, enter `terraform init` to initialize the working directory.

It reads the provider if the name follows the convention `terraform-provider-[name]`:

```
root@mail:/home/terraform# terraform init
Initializing the backend...
Terraform has been successfully initialized!
You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.
If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
```



**7. Run terraform -v to verify the version of loaded provider module:**

```
root@mail:/home/terraform# terraform -v
Terraform v0.11.14
+ provider.fortios v1.0.0
```

**8. Enter terraform plan to parse the configuration file and read from the FortiGate configuration to see what Terraform changes:**

This example create a static route and updates the DNS address. You can see that Terraform reads the DNS addresses from the FortiGate and then lists them.

```
root@mail:/home/terraform# terraform plan
Refreshing Terraform state in-memory prior to plan...
The refreshed state will be used to calculate this plan, but will not be
persisted to local or remote state storage.
fortios_networking_route_static.test1: Refreshing state... (ID: 2)
fortios_system_setting_dns.test1: Refreshing state... (ID: 208.91.112.53)

```

An execution plan has been generated and is shown below.  
Resource actions are indicated with the following symbols:

```
+ create
~ update in-place
Terraform will perform the following actions:
+ fortios_networking_route_static.test1
id: <computed>
blackhole: "disable"
comment: "Terraform test"
device: "port2"
distance: "22"
dst: "110.2.2.122/32"
gateway: "2.2.2.2"
priority: "3"
weight: "3"
~ fortios_system_setting_dns.test1
primary: "208.91.112.53" => "172.16.95.16"
secondary: "208.91.112.22" => "8.8.8.8"
Plan: 1 to add, 1 to change, 0 to destroy.

```

Note: You didn't specify an "-out" parameter to save this plan, so Terraform can't guarantee that exactly these actions will be performed if "terraform apply" is subsequently run.



If you are running terraform-provider-fortios 1.1.0, you may see the following error:

```
Error: Error getting CA Bundle, CA Bundle should be set when
insecure is false.
```

In this case, add the following line to the FortiOS provider configuration in the test.tf file:

```
insecure = "true"
```

**9. Enter terraform apply to continue the configuration:**

```
root@mail:/home/terraform# terraform apply
fortios_system_setting_dns.test1: Refreshing state... (ID: 208.91.112.53)
fortios_networking_route_static.test1: Refreshing state... (ID: 2)
An execution plan has been generated and is shown below.
Resource actions are indicated with the following symbols:
+ create
```

```

~ update in-place
Terraform will perform the following actions:
+ fortios_networking_route_static.test1
id: <computed>
blackhole: "disable"
comment: "Terraform test"
device: "port2"
distance: "22"
dst: "110.2.2.122/32"
gateway: "2.2.2.2"
priority: "3"
weight: "3"
~ fortios_system_setting_dns.test1
primary: "208.91.112.53" => "172.16.95.16"
secondary: "208.91.112.22" => "8.8.8.8"
Plan: 1 to add, 1 to change, 0 to destroy.
Do you want to perform these actions?
Terraform will perform the actions described above.
Only 'yes' will be accepted to approve.
Enter a value: yes
fortios_networking_route_static.test1: Creating...
blackhole: "" => "disable"
comment: "" => "Terraform test"
device: "" => "port2"
distance: "" => "22"
dst: "" => "110.2.2.122/32"
gateway: "" => "2.2.2.2"
priority: "" => "3"
weight: "" => "3"
fortios_system_setting_dns.test1: Modifying... (ID: 208.91.112.53)
primary: "208.91.112.53" => "172.16.95.16"
secondary: "208.91.112.22" => "8.8.8.8"
fortios_networking_route_static.test1: Creation complete after 0s (ID: 2)
fortios_system_setting_dns.test1: Modifications complete after 0s (ID: 172.16.95.16)
Apply complete! Resources: 1 added, 1 changed, 0 destroyed.

```

The FortiGate is now configured according to the configuration file.

10. To change or delete something in the future, edit the configuration file and then apply it again. In supported cases, it deletes, adds, or updates new entries as configured. For instance, in this example you can remove the static route and revert the DNS address to its original configuration by changing the .tf file:

**a. Edit the configuration file:**

```

Configure the FortiOS Provider
provider "fortios" {
 hostname = "10.6.30.5"
 token = "17b*****63ck"
}
resource "fortios_system_setting_dns" "test1" {
 primary = "208.91.112.53"
 secondary = "208.91.112.22"
}
#resource "fortios_networking_route_static" "test1" {
dst = "110.2.2.122/32"
gateway = "2.2.2.2"
blackhole = "disable"
distance = "22"

```

```
weight = "3"
priority = "3"
device = "port2"
comment = "Terraform test"
#}
```

- b. Entering `terraform apply` deletes the static route that is commented out of the configuration file, and reverts the DNS address to the old address:

```
root@mail:/home/terraform# terraform apply
fortios_system_setting_dns.test1: Refreshing state... (ID: 172.16.95.16)
fortios_networking_route_static.test1: Refreshing state... (ID: 2)
An execution plan has been generated and is shown below.
Resource actions are indicated with the following symbols:
~ update in-place
- destroy
Terraform will perform the following actions:
- fortios_networking_route_static.test1
~ fortios_system_setting_dns.test1
primary: "172.16.95.16" => "208.91.112.53"
secondary: "8.8.8.8" => "208.91.112.22"
Plan: 0 to add, 1 to change, 1 to destroy.
Do you want to perform these actions?
Terraform will perform the actions described above.
Only 'yes' will be accepted to approve.
Enter a value: yes
fortios_networking_route_static.test1: Destroying... (ID: 2)
fortios_system_setting_dns.test1: Modifying... (ID: 172.16.95.16)
primary: "172.16.95.16" => "208.91.112.53"
secondary: "8.8.8.8" => "208.91.112.22"
fortios_networking_route_static.test1: Destruction complete after 0s
fortios_system_setting_dns.test1: Modifications complete after 0s (ID: 208.91.112.53)
Apply complete! Resources: 0 added, 1 changed, 1 destroyed.
```

## Troubleshooting

Use the HTTPS daemon debug to begin troubleshooting why a configuration was not accepted:

```
diagnose debug enable
diagnose debug application httpsd -1
[httpsd 333 - 1560376452 info] ap_invoke_handler[569] -- new request (handler='api_cmdb_v2-
handler', uri='/api/v2/cmdb/router/static/2', method='GET')
[httpsd 23616 - 1560376452 info] handle_cli_req_v2_vdom[2034] -- new CMDB API request
(vdom='root',user='test')
[httpsd 333 - 1560376452 info] ap_invoke_handler[573] -- User-Agent: Go-http-client/1.1
[httpsd 23616 - 1560376452 info] api_cmdb_request_init_by_path[1438] -- new CMDB query
(path='system',name='dns')
[httpsd 333 - 1560376452 info] ap_invoke_handler[576] -- Source: 10.6.30.55:49666
Destination: 10.6.30.5:443
[httpsd 333 - 1560376452 info] api_cmdb_v2_handler[2132] -- received api_cmdb_v2_request
from '10.6.30.55'
[httpsd 23616 - 1560376452 info] api_cmdb_select_etag[2146] -- ETag check for system.dns
[httpsd 23616 - 1560376452 info] api_return_cmdb_revision[837] -- ETag check for system.dns
[httpsd 23616 - 1560376452 info] api_add_etag[918] -- no If-None-Match header
[httpsd 333 - 1560376452 warning] api_access_check_for_api_key[965] -- API Key request
authorized for test from 10.6.30.55.
```

```
[httpsd 23616 - 1560376452 info] api_return_cmdb_revision[837] -- ETag check for system.dns
[httpsd 333 - 1560376452 info] api_store_parameter[239] -- add API parameter 'access_token'
(type=string)
[httpsd 333 - 1560376452 info] handle_cli_req_v2_vdom[2034] -- new CMDB API request
(vdom='root',user='test')
[httpsd 333 - 1560376452 info] api_cmdb_request_init_by_path[1438] -- new CMDB query
(path='router',name='static')
[httpsd 333 - 1560376452 info] api_cmdb_request_init_by_path[1467] -- querying CMDB entry
(mkey='2')
[httpsd 333 - 1560376452 info] api_cmdb_select_etag[2146] -- ETag check for router.static
[httpsd 333 - 1560376452 info] api_return_cmdb_revision[837] -- ETag check for router.static
[httpsd 333 - 1560376452 info] api_add_etag[918] -- no If-None-Match header
[httpsd 333 - 1560376452 info] api_cmdb_v2_object_select[843] -- filter by master key (seq-
num)
[httpsd 23616 - 1560376452 info] ap_invoke_handler[592] -- request completed (handler='api_
cmdb_v2-handler' result==0)
```



The REST API 403 error means that your administrator profile does not have sufficient permissions.

The REST API 401 error means that you do not have the correct token or trusted host.

## PF SR-IOV driver support

Physical Function (PF) SR-IOV drivers for i40e and ixgbe interfaces in virtual environments are supported.

PF provides the ability for PCI Passthrough, but requires an entire Network Interface Card (NIC) for a VM. It can usually achieve greater performance than a Virtual Function (VF) based SR-IOV. PF is also expensive; while VF allows one NIC to be shared among multiple guests VMs, PF is allocated to one port on a VM.

The supported driver versions are:

- ixgbe: 5.3.7
- ixgbev: 4.3.5
- i40e: 2.4.10
- i40evl 3.5.13



All tools and software utilities for UEFI 1.X have been removed from 6.2.0 and later releases. Update to UEFI 2.x to use the UEFI tools or software utilities.

Configuration to use PF or VF is done on the hypervisor, and is not configured on the FortiGate.

To check what driver is being used on the FortiGate:

```
diagnose hardware deviceinfo nic port2
Name: port2
Driver: i40e
Version: 2.4.10
Bus: 0000:03:00.0
Hwaddr: 3c:fd:fe:1e:98:02
Permanent Hwaddr:3c:fd:fe:1e:98:02
```

```
State: up
Link: up
Mtu: 1500
Supported: auto 1000full 10000full
Advertised: auto 1000full 10000full
Auto: disabled
Rx packets: 0
Rx bytes: 0
Rx compressed: 0
...
```

# Troubleshooting

This section is intended for administrators with super\_admin permissions who require assistance with basic and advanced troubleshooting. Admins with other types of permissions may not be able to perform all of the tasks in this section.

This section contains the following troubleshooting topics:

- [Troubleshooting methodologies on page 1680](#)
- [Troubleshooting scenarios on page 1684](#)
  - [Checking the system date and time on page 1685](#)
  - [Checking the hardware connections on page 1686](#)
  - [Checking FortiOS network settings on page 1687](#)
  - [Troubleshooting CPU and network resources on page 1690](#)
  - [FortiGuard server settings on page 1724](#)
  - [Troubleshooting high CPU usage on page 1691](#)
  - [Checking the modem status on page 1695](#)
  - [Running ping and traceroute on page 1696](#)
  - [Checking the logs on page 1700](#)
  - [Verifying routing table contents in NAT mode on page 1700](#)
  - [Verifying the correct route is being used on page 1701](#)
  - [Verifying the correct firewall policy is being used on page 1701](#)
  - [Checking the bridging information in transparent mode on page 1702](#)
  - [Checking wireless information on page 1703](#)
  - [Performing a sniffer trace \(CLI and packet capture\) on page 1704](#)
  - [Debugging the packet flow on page 1707](#)
  - [Testing a proxy operation on page 1710](#)
  - [Displaying detail Hardware NIC information on page 1710](#)
  - [Performing a traffic trace on page 1713](#)
  - [Using a session table on page 1714](#)
  - [Finding object dependencies on page 1717](#)
  - [Diagnosing NPU-based interfaces on page 1718](#)
  - [Running the TAC report on page 1719](#)
  - [Other commands on page 1719](#)
  - [FortiGuard troubleshooting on page 1722](#)
- [Additional resources on page 1725](#)

## Troubleshooting methodologies

The sections in this topic provide an overview of how to prepare to troubleshoot problems in FortiGate. They include verifying your user permissions, establishing a baseline, defining the problem, and creating a plan.

## Verify user permissions

Before you begin troubleshooting, verify the following:

- You have administrator privileges for the FortiGate.
- The FortiGate is integrated into your network.
- The operation mode is configured.
- The system time, DNS settings, administrator password, and network interfaces are configured.
- Firmware, FortiGuard AntiVirus, FortiGuard Application Control, and FortiGuard IPS are up to date.



If you are using a FortiGate that has virtual domains (VDOMs) enabled, you can often troubleshoot within your own VDOM. However, you should inform the super\_admin for the FortiGate that you will be performing troubleshooting tasks.

You may also need access to other networking equipment, such as switches, routers, and servers, to carry out tests. If you do not have access to this equipment, contact your network administrator for assistance.

## Establish a baseline

FortiGate operates at all layers of the OSI model. For this reason, troubleshooting can be complex. Establishing baseline parameters for your system before a problem occurs helps to reduce the complexity when you need to troubleshoot.

A best practice is to establish and record the normal operating status. Regular operation data shows trends, and allows you to see where changes occur when problems arise. You can gather this data by using logs and SNMP tools to monitor the system performance or by regularly running information gathering commands and saving the output.



You should back up your FortiOS configuration on a regular basis even when you are not troubleshooting. You can restore the backed up configuration as needed to save time recreating it from the factory default settings.

Use the following CLI commands to obtain normal operating data for a FortiGate:

<code>get system status</code>	Displays firmware versions and FortiGuard engine versions, and other system information.
<code>get system performance status</code>	Displays CPU and memory states, average network usage, average sessions and session setup rate, viruses caught, IPS attacks blocked, and uptime.
<code>get hardware memory</code>	Displays information about memory.
<code>get system session status</code>	Displays total number of sessions.
<code>get router info routing-table all</code>	Displays all the routes in the routing table, including their type, source, and other useful data.
<code>get ips session</code>	Displays memory used and maximum amount available to IPS as well as counts

<code>get webfilter ftgd-statistics</code>	Displays a list of FortiGuard related counts of status, errors, and other data.
<code>diagnose sys session list</code>	Displays the list of current detailed sessions.
<code>show sys dns</code>	Displays the configured DNS servers.
<code>diagnose sys ntp status</code>	Displays information about NTP servers.

You can run any commands that apply to your system for information gathering. For example, if you have active VPN connections, use the `get vpn` series of commands to get more information about them.

Use `execute tac report` to get an extensive snapshot of your system. This command runs many diagnostic commands for specific configurations. It also records the current state of each feature regardless of the features deployed on your FortiGate. If you need to troubleshoot later, you can run the same command again and compare the differences to identify any suspicious output.

## Define the problem

The following questions are intended to compare the current behavior of the FortiGate with normal operations to help you define the problem. Be specific with your answers. After you define the problem, search for a solution in the troubleshooting scenarios section, and then create a plan to resolve it.


<b>What is the problem?</b>	The problem being observed may not be the actual problem. You should determine where the problem lies before starting to troubleshoot the FortiGate.
<b>Was the device working before?</b>	If the device never worked, it might be defective. For more information, see <a href="#">Troubleshooting your installation on page 51</a> .
<b>Can the problem be reproduced?</b>	If the problem is intermittent, it may be dependent on system load. Intermittent problems are challenging to troubleshoot because they are difficult to reproduce.
<b>What has changed?</b>	Use the FortiGate event log to identify possible configuration changes. There may be changes in the operating environment. For example, there might be a gradual increase in load as more sites are forwarded through the firewall. If something has changed, roll back the change and assess the impact.
<b>What is the scope of the problem?</b>	After you isolate the problem, determine what applications, users, devices, and operating systems the problem affects. The following questions are intended to narrow the scope of the problem and identify what to check during troubleshooting. The more factors you can eliminate, the less you need to check. For this reason, be as specific and accurate as possible when gathering information. <ul style="list-style-type: none"> <li>• What is not working?</li> <li>• Is more than one thing not working?</li> <li>• Is it partly working? If so, what parts are working?</li> <li>• Is it a connectivity issue for the entire device, or is there an application that isn't reaching the Internet?</li> <li>• Where did the problem occur?</li> <li>• When did the problem occur and to which users or groups of users?</li> </ul>



- What components are involved?
- What applications are affected?
- Can you use a packet sniffer to trace the problem?
- Can you use system debugging or look in the session table to trace the problem?
- Do any of the log files indicate a failure has occurred?

## Create a troubleshooting plan

After you define the problem and its scope, develop a troubleshooting plan.

<b>Create checklist</b>	<p>Make a list all the possible causes of the problem and how you can test for each cause.</p> <p>Create a checklist to keep track of what has been tried and what is left to test. Checklists are useful when more than one person is performing troubleshooting tasks.</p>
<b>Obtain the required equipment</b>	<p>Testing your solution may require additional networking equipment, computers, or other devices.</p> <p>Network administrators usually have additional networking equipment available to loan you, or a lab where you can bring the FortiGate unit to test.</p> <p>If you do not have access to equipment, check for shareware applications that can perform the same tasks. Often, there are software solutions you can use when hardware is too expensive.</p>
<b>Consult Fortinet troubleshooting resources</b>	<p>After the checklist is created, refer to the troubleshooting scenarios sections to assist with implementing your plan. See <a href="#">Troubleshooting scenarios on page 1684</a>.</p>
<b>Gather information for technical support</b>	<p>If you still require technical assistance after the plan is implemented, be prepared to provide Fortinet technical support with following information:</p> <ul style="list-style-type: none"> <li>• Firmware build version (use the <code>get system status</code> command)</li> <li>• Network topology diagram</li> <li>• Recent configuration file</li> <li>• Recent debug log (optional)</li> <li>• Summary of troubleshooting steps you have taken and the results.</li> </ul> <hr/> <div>  <p>Do not provide the output from the <code>exec tac</code> report unless the support team requests it. The output from this command is very large and is not required in many cases.</p> </div>
<b>Contact technical support</b>	<p>Before contacting technical support, ensure you have login access (preferably with full read/write privileges) to all networking devices that could be relevant to troubleshooting.</p> <p>If you are using VMs, be prepared to have someone who can log in to the virtual hosting platform in case it is necessary to check and possibly modify resource allocation.</p>

For information about contacting technical support, go to [FortiCare Support Service](#) page.

## Troubleshooting scenarios

The following table is intended to help you diagnose common problems and provides links to the corresponding troubleshooting topics:

Problem	Probable cause	Recommended action
<b>Hardware connections</b>	<ul style="list-style-type: none"> <li>Are all of the cables and interfaces connected properly?</li> <li>Is the LED for the interface green?</li> </ul>	<a href="#">Checking the hardware connections on page 1686</a>
<b>FortiOS network settings</b>	<ul style="list-style-type: none"> <li>If you are having problems connecting to the management interface, is your protocol enabled on the interface for administrative access?</li> <li>Does the interface have an IP address?</li> </ul>	<a href="#">Checking FortiOS network settings on page 1687</a>
<b>CPU and memory resources</b>	<ul style="list-style-type: none"> <li>Is the CPU running at almost 100 percent usage?</li> <li>Is your FortiGate running low on memory?</li> </ul>	<a href="#">Troubleshooting CPU and network resources on page 1690</a>
<b>Modem status</b>	<ul style="list-style-type: none"> <li>Is the modem connected?</li> <li>Are there PPP issues?</li> </ul>	<a href="#">Checking the modem status on page 1695</a>
<b>Ping and traceroute</b>	Is the FortiGate experiencing complete packet loss?	<a href="#">Running ping and traceroute on page 1696</a>
<b>Logs</b>	Do you need to identify a problem?	<a href="#">Checking the logs on page 1700</a>
<b>Contents of the routing table (in NAT mode)</b>	<ul style="list-style-type: none"> <li>Are there routes in the routing table for default and static routes?</li> <li>Do all connected subnets have a route in the routing table?</li> <li>Does a route have a higher priority than it should?</li> </ul>	<a href="#">Verifying routing table contents in NAT mode on page 1700</a>
<b>Traffic routes</b>	Is the traffic routed correctly?	<a href="#">Verifying the correct route is being used on page 1701</a>
<b>Firewall policies</b>	Is the correct firewall policy applied to the expected traffic?	<a href="#">Verifying the correct firewall policy is being used on page 1701</a>
<b>Bridging information in transparent mode</b>	Are you having problems in transparent mode?	<a href="#">Checking the bridging information in transparent mode on page 1702</a>
<b>Firewall session</b>	<ul style="list-style-type: none"> <li>Are there active firewall sessions?</li> </ul>	<a href="#">Using a session table on page 1714</a>

Problem	Probable cause	Recommended action
<b>list</b>		
<b>Wireless Network</b>	Is the wireless network working properly?	<a href="#">Checking wireless information on page 1703</a>
<b>FortiGuard connectivity</b>	Is the FortiGate communicating properly with FortiGuard?	<a href="#">Verifying connectivity to FortiGuard on page 1722</a>
<b>Sniffer trace</b>	<ul style="list-style-type: none"> <li>Is traffic entering the FortiGate? Does the traffic arrive on the expected interface?</li> <li>Is the ARP resolution correct for the next-hop destination?</li> <li>Is the traffic exiting the FortiGate to the destination as expected?</li> <li>Is the FortiGate sending traffic back to the originator?</li> </ul>	<a href="#">Performing a sniffer trace (CLI and packet capture) on page 1704</a>
<b>Packet flow</b>	Is traffic entering or leaving the FortiGate as expected?	<a href="#">Debugging the packet flow on page 1707</a>

## Checking the system date and time

The system date and time are important for FortiGuard services, logging events, and sending alerts. The wrong time makes the log entries confusing and difficult to use.

When possible, use Network Time Protocol (NTP) to set the date and time. This is an automatic method that does not require manual intervention. However, you must ensure that the port is allowed through the firewalls on your network. FortiToken synchronization requires NTP in many situations.

For information about setting the system date and time, see [Setting the system time on page 634](#).

### To view and configure the date and time in the GUI:

1. Go to *Dashboard > Status*. The date and time are displayed in the *System Information* widget, next to *System Time*.
2. Go to *System > Settings*.
3. In the *System Time* section, select *NTP*, and then configure the *Time Zone*, and *Set Time* settings as required.

### To view the date and time in the CLI:

```
execute date
execute time
```

### To configure the date and time in the CLI:

Use the `set timezone ?` command to display a list of timezones and the integers that represent them.

```
config system global
 set timezone <integer>
end
config system ntp
 set type custom
```

```

config ntpserver
 edit 1
 set server "ntp1.fortinet.net"
 next
 edit 2
 set server "ntp2.fortinet.net"
 next
end
set ntpsync enable
set syncinterval 60
end

```

## Checking the hardware connections

If traffic is not flowing from the FortiGate, there may be a problem with the hardware connection.

### To check hardware connections:

1. Ensure the network cables are plugged into the interfaces.
2. Verify the LED connection lights for the network cables indicate there is a connection. The lights are typically green when there is a connection.
3. Change the cable when:
  - The cable or its connector are damaged.
  - You are unsure of the type or quality of the cable, such as straight through or crossover.
  - You see exposed wires at the connector.
4. Connect the FortiGate to different hardware.
5. Go to *Network > Interfaces* to ensure the link status for the interface is set to *Up*.  
The link status is based on the physical connection and cannot be set in FortiOS.

### To enable an interface in the GUI:

You should still perform basic software connectivity tests to ensure complete connectivity even if there was problem with the hardware connection. The interface might also be disabled, or its *Status* might be set to *Down*. See [Interfaces on page 315](#).

1. Go to *Network > Interfaces*.
2. Select an interface, such as *Port1*, and click *Edit*.
3. In the *Miscellaneous* area, next to *Status*, click *Enabled*.
4. Click *OK*.

### To enable an interface in the CLI:

```

config system interface
 edit port1
 set status up
 next
end

```

## Checking FortiOS network settings

Check the FortiOS network settings if you have problems connecting to the management interface. FortiOS network settings include, interface settings, DNS Settings, and DHCP settings.

### Interface settings

If you can access the FortiGate with the management cable only, you can view the interface settings in the GUI.

#### To view the interface settings in the GUI:

1. Go to *Network > Interfaces*.
2. Select an interface and click *Edit*.
3. Check the following interfaces to ensure they are not blocking traffic.

Setting	Description
<b>Link Status</b>	The status is <i>Up</i> when a valid cable is plugged in. The status is <i>Down</i> when an invalid cable is plugged in.  The Link Status is shown physically by the connection LED for the interface. If the LED is green, the connection is good. If Link Status is <i>Down</i> , the interface does not work.  Link status also appears in the <i>Network &gt; Interfaces</i> page by default.
<b>Addressing mode</b>	Do not use <i>DHCP</i> if you do not have a DHCP server. You will not be able to log into an interface in DHCP mode as it will not have an IP address.
<b>IP/Network Mask</b>	An interface requires an IP address to connect to other devices. Ensure there is a valid IP address in this field. The one exception is when <i>DHCP</i> is enabled for this interface to get its IP address from an external DHCP server.
<b>IPv6 address</b>	The same protocol must be used by both ends to complete the connection. Ensure this interface and the remote connection are both using IPv4 or both are using IPv6 addresses.
<b>Administrative access</b>	If no protocols are selected, you will have to use the local management cable to connect to the unit. If you are using IPv6, configure the IPv6 administrative access protocols.
<b>Status</b>	Ensure the status is set to <i>Up</i> or the interface will not work.

#### To display the internal interface settings in the CLI:

```
FGT# show system interface <interface_name>
```

#### To view the list of possible interface settings:

```
config system interface
 edit <interface_name>
 get
 end
```

## DNS settings

### To view DNS settings in the GUI:

Go to *Network > DNS*.

You can trace many networking problems back to DNS issues. Check the following items:

1. Are there values for both the *Primary DNS server* and *Secondary DNS server* fields.
2. Is the *Local Domain Name* correct?
3. Are you using IPv6 addressing? If so, are the IPv6 DNS settings correct?
4. Are you using Dynamic DNS (DDNS)? If so, is it using the correct server, credentials, and interface?
5. Can you contact both DNS servers to verify the servers are operational?
6. If an interface addressing mode is set to DHCP and is set to override the internal DNS, is that interface receiving a valid DNS entry from the DHCP server? Is it a reasonable address and can it be contacted to verify it is operational?
7. Are there any DENY security policies that need to allow DNS?
8. Can any internal device perform a successful traceroute to a location using the FQDN?

### DHCP server settings

DHCP servers are common on internal and wireless networks. The DHCP server will cause problems if it is not configured correctly.

### To view DHCP server settings in the GUI:

1. Go to *Network > Interfaces*.
2. Select an interface, and click *Edit*.

### Check the following items:

1. Is the DHCP server enabled?
2. Is the DHCP server entry set to *Relay*? If so, verify there is another DHCP server to which requests can be relayed. Otherwise, set it to *Server*.
3. Does the DHCP server use a valid IP address range? Are other devices using the addresses? If one or more devices are using IP addresses in this range, you can use the IP reservation feature to ensure the DHCP server does not use these addresses. See [DHCP server on page 400](#)
4. Is there a gateway entry? If not, add a gateway entry to ensure that the server's clients have a default route.
5. Is the system DNS setting being used? A best practice is to avoid confusion by using the system DNS whenever possible. However, you can specify up to three custom DNS servers, and you should use all three entries for redundancy.



There are some situations, such as a new wireless interface, or during the initial FortiGate configuration, where interfaces override the system DNS entries. When this happens, it often shows up as intermittent Internet connectivity.

To fix the problem, go to *Network > DNS*, and enable *Use FortiGuard Servers*.

## Checking CPU and memory resources

Check the CPU and memory resources when the FortiGate is not working, the network is slow, or there is a reduced firewall session setup rate. All processes share the system resources in FortiOS, including CPU and memory.

### To view system resources in the GUI:

Go to *Dashboard > Status*.

The resource information is located in the *CPU* and *Memory* widgets. For information, see [Dashboard on page 58](#).

### To view system resources in the CLI:

```
get system performance status
```

### Sample output:

```
FGT# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU2 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU3 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 4050332k total, 527148k used (13%), 3381312k free (83%), 141872k freeable (3%)
Average network usage: 41 / 28 kbps in 1 minute, 54 / 44 kbps in 10 minutes, 42 / 34 kbps
in 30 minutes
Average sessions: 33 sessions in 1 minute, 48 sessions in 10 minutes, 38 sessions in 30
minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second
in last 10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 0 days, 22 hours, 59 minutes
```

The first line of the output shows the CPU usage by category:

```
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
```

The second line of the output shows the memory usage:

```
Memory: 4050332k total, 527148k used (13%), 3381312k free (83%), 141872k freeable (3%)
```

Memory usage should not exceed 90%. Using too much memory prevents some processes from functioning properly. For example, if the system is running low on memory, antivirus scanning enters into *failopen* mode where it drops connections or bypasses the antivirus system.

Other lines of output, such as average network usage, average session setup rate, viruses caught, and IPS attacks blocked, help determine why system resource usage is high.

For example:

- A high average network usage may indicate high traffic processing on the FortiGate,
- A very low or zero, average session setup rate may indicate the proxy is overloaded and unable to do its job.

## Troubleshooting CPU and network resources

### FortiGate has stopped working

If the FortiGate has stopped working, the first line of the output will look similar to this:

```
CPU states: 0% user 0% system 0% nice 100% idle
```

### Network is slow

If your network is running slow, the first line of the output will look similar to this:

```
CPU states: 1% user 98% system 0% nice 1% idle
```

This example shows that all of the CPU is being used by system processes, and the FortiGate is overloaded. When overloading occurs, it is possible a process such as `scanunitid` is using all the resources to scan traffic. In this case you need to reduce the amount of traffic being scanned by blocking unwanted protocols, configuring more security policies to limit scanning to certain protocols, or similar actions.

It is also possible a hacker has accessed your network and is overloading it with malicious activity, such as running a spam server or using zombie PCs to attack other networks on the Internet.

You can use the following command to investigate the problem with the CPU:

```
get system performance top
```

This command shows all of the top processes that are running on the FortiGate and their CPU usage. The process names are on the left. If a process is using most of the CPU cycles, investigate it to determine whether the activity is normal.

### Reduced firewall session setup rate

A reduced firewall session setup rate can be caused by a lack of system resources on the FortiGate, or reaching the session count limit for a VDOM.



As a best practice, administrators should record the session setup rate during normal operation to establish a baseline to help define a problem when you are troubleshooting.

---

The session setup rate appears in the `average sessions` section of the output.

A reduced firewall session setup rate will look similar to this:

```
Average sessions: 80 sessions in 1 minute, 30 sessions in 10 minutes, 42 sessions in 30
minutes
```

```
Average session setup rate: 3 sessions per second in last 1 minute, 0 sessions per second in
last 10 minutes, 0 sessions per second in last 30 minutes
```

In the example above, there were 80 sessions in 1 minute, or an average of 3 sessions per second.

The values for `10 minutes` and `30 minutes` allow you to take a longer average for a more reliable value if your FortiGate is working at maximum capacity. The smallest FortiGate can have 1,000 sessions established per second across the unit.





The session setup rate is a global command. If you have multiple VDOMs configured with many sessions in each VDOM, the session setup rate per VDOM will be slower than if there are no VDOMs configured.

## High memory usage

As with any system, a FortiGate has limited hardware resources, such as memory, and all processes running on the FortiGate share the memory. Each process uses more or less memory, depending on its workload. For example, a process usually uses more memory in high traffic situations. If some processes use all of the available memory, other processes will not be able to run.

When high memory usage occurs, the services may freeze up, connections may be lost, or new connections may be refused.

If you see high memory usage in the *Memory* widget, the FortiGate may be handling high traffic volumes. Alternatively, the FortiGate may have problems with connection pool limits that are affecting a single proxy. If the FortiGate receives large volumes of traffic on a specific proxy, the unit may exceed the connection pool limit. If the number of free connections within a proxy connection pool reaches zero, issues may occur.

### To view current memory usage information in the CLI:

```
diagnose hardware sysinfo memory
```

### Sample output:

```
total: used: free: shared: buffers: cached: shm:
Mem: 2074185728 756936704 1317249024 0 20701184 194555904 161046528
Swap: 0 0 0
MemTotal: 2025572 kB
MemFree: 1286376 kB
MemShared: 0 kB
Buffers: 20216 kB
Cached: 189996 kB
SwapCached: 0 kB
Active: 56644 kB
Inactive: 153648 kB
HighTotal: 0 kB
HighFree: 0 kB
LowTotal: 2025572 kB
LowFree: 1286376 kB
SwapTotal: 0 kB
SwapFree: 0 kB
```

## Troubleshooting high CPU usage

Connection-related problems may occur when FortiGate's CPU resources are over extended. This occurs when you deploy too many FortiOS features at the same time.

## Examples of CPU intensive features:

- VPN high-level encryption
- Intensive scanning of all traffic
- Logging all traffic and packets
- Dashboard widgets that frequently perform data updates

See [Execute a CLI script based on CPU and memory thresholds on page 264](#) for information on customizing the CPU use threshold.

## Determining the current level of CPU usage

You can view CPU usage levels in the GUI or CLI. For precise usage values for both overall usage and specific processes, use the CLI.

### To view CPU usage in the GUI:

Go to *Dashboard > Status*. Real-time CPU usage information is located in the *CPU* widget.

### To view CPU usage in the CLI:

```
diagnose sys top
```

### Sample output:

```
Run Time: 86 days, 0 hours and 10 minutes
0U, 0N, 0S, 100I, 0WA, 0HI, 0SI, 0ST; 3040T, 2437F
bcm.user 93 S < 3.1 0.4
httpsd 18922 S 1.5 0.5
httpsd 19150 S 0.3 0.5
newcli 20195 R 0.1 0.1
cmdbsvr 115 S 0.0 0.8
pyfcgid 20107 S 0.0 0.6
forticron 146 S 0.0 0.5
httpsd 139 S 0.0 0.5
cw_acd 166 S 0.0 0.5
miglogd 136 S 0.0 0.5
pyfcgid 20110 S 0.0 0.4
pyfcgid 20111 S 0.0 0.4
pyfcgid 20109 S 0.0 0.4
httpsd 20192 S 0.0 0.4
miglogd 174 S 0.0 0.4
miglogd 175 S 0.0 0.4
fgfmd 165 S 0.0 0.3
newcli 20191 S 0.0 0.3
initXXXXXXXXXX 1 S 0.0 0.3
httpsd 184 s 0.0 0.3
```

The following table explains the codes in the second line of the output:

Code	Description
U	Percentage of user space applications that are currently using the CPU
N	Percentage of time that the CPU spent on low priority processes since the last shutdown
S	Percentage of system processes (or kernel processes) that are using the CPU
I	Percentage of idle CPU resources
WA	Percentage of time that the CPU spent waiting on IO peripherals since the last shutdown
HI	Percentage of time that the CPU spent handling hardware interrupt routines since the last shutdown
SI	Percentage of time that the CPU spent handling software interrupt routines since the last shutdown
ST	steal time Percentage of time a virtual CPU waits for the physical CPU when the hypervisor is servicing another virtual processor
T	Total FortiOS system memory in MB
F	Free memory in MB

Each additional line of the command output displays information specific to processes running on the FortiGate unit. For example, the sixth line of the output is: `newcli 20195 R 0.1 0.1`

The following table describes the data in the sixth line of the output:

Item	Description
<code>newcli</code>	The process name. Other process names can include <code>ipsengine</code> , <code>sshd</code> , <code>cmdbsrv</code> , <code>httpsd</code> , <code>scanunitd</code> , and <code>miglogd</code> . Duplicate process names indicate that separate instances of that process that are running.
<code>20195</code>	The process ID, which can be any number.
<code>R</code>	Current state of the process. The process state can be: <ul style="list-style-type: none"> <li>• R - running</li> <li>• S - sleep</li> <li>• Z - zombie</li> <li>• D - disk sleep</li> </ul>
<code>0.1</code>	The percentage of CPU capacity that the process is using. CPU usage can range from 0.0 for a process that is sleeping to higher values for a process that's taking a lot of CPU time.
<code>0.1</code>	The amount of memory that the process is using. Memory usage can range from 0.1 to 5.5 and higher.

You can use the following single-key commands when running `diagnose sys top`:

- `q` to quit and return to the normal CLI prompt.
- `p` to sort the processes by the amount of CPU that the processes are using.
- `m` to sort the processes by the amount of memory that the processes are using.

The output only displays the top processes that are running. For example, if 20 processes are listed, they are the top 20 processes currently running, sorted by either CPU or memory usage. You can configure the number of processes displayed, using the following CLI command:

```
diagnose sys top <integer_seconds> <integer_maximum_lines>
```

Where:

- `<integer_seconds>` is the delay in seconds (default is 5)
- `<integer_maximum_lines>` is the maximum number of lines (or processes) to list (default is 20)

## Determining which features are using the most CPU resources

You can use the CLI to view the top few processes that are currently running and using the most CPU resources.

### To view processes using the most CPU resources:

```
get system performance top
```

The entries at the top are using the most CPU resources. The second column from the right shows CPU usage by percentage. Note which processes are using the most resources and try to reduce their CPU load.

Processes you will see include:

- `ipsengine`: the IPS engine that scans traffic for intrusions
- `scanunitd`: antivirus scanner
- `httpsd`: secure HTTP
- `iked`: internet key exchange (IKE) in use with IPsec VPN tunnels
- `newcli`: active whenever you're accessing the CLI
- `sshd`: there are active secure socket connections
- `cmdbsrv`: the command database server application

Go to the features that are at the top of the list and look for evidence of CPU overuse. Generally, the monitor for a feature is a good place to start.

## Checking for unnecessary CPU “wasters”

These are some best practices that will reduce your CPU usage, even if the FortiGate is not experiencing high CPU usage. Note that if the following information instructs you to turn off a feature that you require, disregard that part of the instructions.

- Use hardware acceleration wherever possible to offload tasks from the CPU. Offloading tasks, such as encryption, frees up the CPU for other tasks.
- Schedule antivirus, IPS, and firmware updates during off-peak hours. These updates do not usually consume CPU resources but they can disrupt normal operation.
- Check the log levels and which events are being logged. This is the severity of the messages that are recorded. Consider going up one level to reduce the amount of logging. Also, if there are events you do not need to monitor, remove them from the list.
- Log to FortiCloud instead of logging to memory or disk. Logging to memory quickly uses up resources and logging to local disk impacts overall performance and reduces the lifetime of the unit. Fortinet recommends logging to FortiCloud to avoid using too much CPU.

- If the disk is almost full, transfer the logs or data off the disk to free up space. When a disk is almost full it consumes a lot of resources to find free space and organize the files.
- If packet logging is enabled on the FortiGate, consider disabling it. When packet logging is enabled, it records every packet that comes through that policy.
- Halt all sniffers and traces.
- Ensure the FortiGate isn't scanning traffic twice. Traffic does not need to be rescanned if it enters the FortiGate on one interface, goes out another, and then comes back in again. Doing so is a waste of resources. However, ensure that traffic truly is being scanned once.
- Reduce the session timers to close unused sessions faster. Enter the following CLI commands, which reduce the default values. Note that, by default, the system adds 10 seconds to `tcp-timewait`.

```
config system global
 set tcp-halfclose-timer 30
 set tcp-halfopen-timer 30
 set tcp-timewait-timer 0
 set udp-idle-timer 60
end
```

- Go to *System > Feature Visibility*, and enable only features that you need.

## SNMP monitoring

When CPU usage is under control, use SNMP to monitor CPU usage. Alternatively, use logging to record CPU and memory usage every 5 minutes.

Once the system is back to normal, you should set up a warning system that sends alerts when CPU resources are used excessively. A common method to do this is using SNMP. SNMP monitors many values in FortiOS and allows you to set high water marks that generate events. You run an application on your computer to watch for and record these events.

### To enable SNMP:

1. Go to *System > SNMP*.
2. Configure an SNMP community.

See [SNMP on page 707](#).



You can use the *System Resources* widget to record CPU usage if SNMP is too complicated. However, the widget only records problems as they happen and will not send you alerts for problems.

## Checking the modem status

You can use the CLI to troubleshoot a modem that is not working properly, or troubleshoot a FortiGate that does not detect the modem.

### To diagnose modem issues in the CLI:

```
diagnose sys modem {cmd | com | detect | history | external-modem | query| reset}
```

You should always run the following command after you connect a USB modem to FortiGate:

```
diagnose sys modem detect
```

Use the following command to view the modem's configuration, vendor and custom product identification number:

```
get system modem
```

Use the following commands to resolve connectivity issues:

- `diagnose debug enable`: Activates the debug on the console
- `diagnose debug application modemd`: Dumps communication between the modem and the unit.
- `diagnose debug application ppp`: Dumps the PPP negotiating messages.
- `execute modem dial`: Displays modem debug output.

The modem diagnose output should not contain errors when initializing. You should also verify the number used to dial into your ISP.

## Running ping and traceroute

Ping and traceroute are useful tools in network troubleshooting. Alone, either tool can determine network connectivity between two points. However, ping can be used to generate simple network traffic that you can view using `diagnose` commands in FortiGate. This combination can be very powerful when you are trying to locate network problems.

Ping and traceroute can also tell you if your computer or network device has access to a domain name server (DNS). Both tools can use IP addresses or device domain names to determine why particular services, such as email or web browsing, may not work properly.



If ping does not work, it may be disabled on at least one of the interface settings and security policies for that interface.

---

Both ping and traceroute require particular ports to be open on firewalls to function. Since you typically use these tools to troubleshoot, you can allow them in the security policies and on interfaces only when you need them. Otherwise, keep the ports disabled for added security.

## Ping

The ping command sends a very small packet to a destination, and waits for a response. The response has a timer that expires when the destination is unreachable.

Ping is part of layer 3 on the OSI Networking Model. Ping sends Internet Control Message Protocol (ICMP) “echo request” packets to the destination, and listens for “echo response” packets in reply. However, many public networks block ICMP packets because ping can be used in a denial of service (DoS) attack (such as Ping of Death or a smurf attack), or by an attacker to find active locations on the network. By default, FortiGate units have ping enabled while broadcast-forward is disabled on the external interface.

### What ping can tell you

Beyond the basic connectivity information, ping can tell you the amount of packet loss (if any), how long it takes the packet to make the round trip, and the variation in that time from packet to packet.

If packet loss is detected, you should investigate the following:

- Possible ECMP, split horizon, or network loops.
- Cabling, to ensure there are no loose connections.

- Verify which security policy was used. To do this:  
Go to *Policy & Objects > IPv4 Policy* or *Policy & Objects > IPv6 Policy* and view the packet count column.

If there is total packet loss, you should investigate the following:

1. Ensure cabling is correct, and all equipment between the two locations is accounted for.
2. Ensure all IP addresses and routing information along the route is configured as expected.
3. Ensure all firewalls, including FortiGate security policies allow PING to pass through.

## How to use ping

Ping syntax is the same for nearly every type of system on a network.

### To ping from a FortiGate unit:

1. Go to *Dashboard*, and connect to the CLI through either telnet or the CLI widget.
2. Enter `exec ping 10.11.101.101` to send 5 ping packets to the destination IP address. There are no options for this command.

#### Sample output:

```
Head_Office_620b # exec ping 10.11.101.101
PING 10.11.101.101 (10.11.101.101): 56 data bytes
64 bytes from 10.11.101.101: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 10.11.101.101: icmp_seq=1 ttl=255 time=0.2 ms
64 bytes from 10.11.101.101: icmp_seq=2 ttl=255 time=0.2 ms
64 bytes from 10.11.101.101: icmp_seq=3 ttl=255 time=0.2 ms
64 bytes from 10.11.101.101: icmp_seq=4 ttl=255 time=0.2 ms

--- 10.11.101.101 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.3 ms
```

### To ping from a Microsoft Windows PC:

1. Open a command window.
2. Enter `ping 10.11.101.100` to ping the default internal interface of the FortiGate with four packets.

Other options include:

- `-t` to send packets until you press `Ctrl+C`
- `-a` to resolve addresses to domain names where possible
- `-n X` to send X ping packets and stop

#### Sample output:

```
C:\>ping 10.11.101.101

Pinging 10.11.101.101 with 32 bytes of data:
Reply from 10.11.101.101: bytes=32 time=10ms TTL=255
Reply from 10.11.101.101: bytes=32 time<1ms TTL=255
Reply from 10.11.101.101: bytes=32 time=1ms TTL=255
Reply from 10.11.101.101: bytes=32 time=1ms TTL=255

Ping statistics for 10.11.101.101:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 10ms, Average = 3ms

### To ping from a Linux PC:

1. Go to a shell prompt.
2. Enter `"ping 10.11.101.101"`.

## Traceroute

Where ping will only tell you if it reached its destination and returned successfully, traceroute shows each step of the journey to its destination and how long each step takes. If ping finds an outage between two points, you can use traceroute to locate exactly where the problem is.

Traceroute works by sending ICMP packets to test each hop along the route. It sends three packets, and then increases the time to live (TTL) setting by one each time. This effectively allows the packets to go one hop farther along the route. This is why most traceroute commands display their maximum hop count before they start tracing the route, which is the maximum number of steps it takes before it declares the destination unreachable. Also, the TTL setting may result in steps along the route timing out due to slow responses. There are many possible reasons for this to occur.

By default, traceroute uses UDP datagrams with destination ports numbered from 33434 to 33534. The traceroute utility may also offer the option to select use of ICMP echo request (type 8) instead, which the Windows tracert utility uses. If you must, allow both protocols inbound through the FortiGate security policies (UDP with ports from 33434 to 33534 and ICMP type 8).

### To track traceroute packets in the GUI:

Go to *Policy & Objects > IPv4 Policy* or *Policy & Objects > IPv6 Policy* (if applicable) and view the packet count column.

This allows you to verify the connection and confirm which security policy the traceroute packets are using.

## What traceroute can tell you

Both ping and traceroute verify connectivity between two points. However, only traceroute shows you each step in the connection path. Also, ping and traceroute use different protocols and ports, so one may succeed where the other fails.

You can verify your DNS connection using traceroute. If you enter an FQDN instead of an IP address for the traceroute, DNS tries to resolve that domain name. If the name isn't resolved, you have DNS issues.

## Using traceroute

The traceroute command varies slightly between operating systems. In Microsoft Windows, the command name is shortened to `"tracert"`. Also, your output lists different domain names and IP addresses along your route.

### To use traceroute on a Microsoft Windows PC:

1. Open a command window.
2. Enter `tracert fortinet.com` to trace the route from the PC to the Fortinet web site.

### Sample output:

```
C:\>tracert fortinet.com
```



```
Tracing route to fortinet.com [208.70.202.225]
over a maximum of 30 hops:
 1 <1 ms <1 ms <1 ms 172.20.120.2
 2 66 ms 24 ms 31 ms 209-87-254-xxx.storm.ca [209.87.254.221]
 3 52 ms 22 ms 18 ms core-2-g0-0-1104.storm.ca [209.87.239.129]
 4 43 ms 36 ms 27 ms core-3-g0-0-1185.storm.ca [209.87.239.222]
 5 46 ms 21 ms 16 ms te3-x.1156.mpd01.cogentco.com [38.104.158.69]
 6 25 ms 45 ms 53 ms te8-7.mpd01.cogentco.com [154.54.27.249]
 7 89 ms 70 ms 36 ms te3-x.mpd01.cogentco.com [154.54.6.206]
 8 55 ms 77 ms 58 ms sl-st30-g0-.sprintlink.net [144.232.9.69]
 9 53 ms 58 ms 46 ms sl-0-3-3-x.sprintlink.net [144.232.19.181]
10 82 ms 90 ms 75 ms sl-x-12-0-1.sprintlink.net [144.232.20.61]
11 122 ms 123 ms 132 ms sl-0-x-0-3.sprintlink.net [144.232.18.150]
12 129 ms 119 ms 139 ms 144.232.20.7
13 172 ms 164 ms 243 ms sl-321313-0.sprintlink.net [144.223.243.58]
14 99 ms 94 ms 93 ms 203.78.181.18
15 108 ms 102 ms 89 ms 203.78.176.2
16 98 ms 95 ms 97 ms 208.70.202.225
```

The first column on the left is the hop count, which can't exceed 30 hops. When that number is reached, the traceroute ends.

The second, third, and fourth columns display how much time each of the three packets takes to reach this stage of the route. These values are in milliseconds and normally vary quite a bit. Typically a value of <1ms indicates a local connection.

The fifth column (farthest to the right) shows the domain name of the device and its IP address, or possibly only the IP address.

### To perform a traceroute on a Linux PC:

1. Go to a command line prompt.
2. Enter "traceroute fortinet.com".

The Linux traceroute output is very similar to the MicroSoft Windows `tracert` output.

### To trace a route from a FortiGate to a destination IP address in the CLI:

```
execute traceroute www.fortinet.com

traceroute to www.fortinet.com (66.171.121.34), 32 hops max, 84 byte packets
 1 172.20.120.2 0.637 ms 0.653 ms 0.279 ms
 2 209.87.254.221 <static-209-87-254-221.storm.ca> 2.448 ms 2.519 ms 2.458 ms
 3 209.87.239.129 <core-2-g0-2.storm.ca> 2.917 ms 2.828 ms 9.324 ms
 4 209.87.239.199 <core-3-bdi1739.storm.ca> 13.248 ms 12.401 ms 13.009 ms
 5 216.66.41.113 <v502.core1.tor1.he.net> 17.181 ms 12.422 ms 12.268 ms
 6 184.105.80.9 <100ge1-2.core1.nyc4.he.net> 21.355 ms 21.518 ms 21.597 ms
 7 198.32.118.41 <ny-paix-gni.twgate.net> 83.297 ms 84.416 ms 83.782 ms
 8 203.160.228.217 <217-228-160-203.TWGATE-IP.twgate.net> 82.579 ms 82.187 ms 82.066 ms
 9 203.160.228.229 <229-228-160-203.TWGATE-IP.twgate.net> 82.055 ms 82.455 ms 81.808 ms
10 203.78.181.2 82.262 ms 81.572 ms 82.015 ms
11 203.78.186.70 83.283 ms 83.243 ms 83.293 ms
12 66.171.127.177 84.030 ms 84.229 ms 83.550 ms
13 66.171.121.34 <www.fortinet.com> 84.023 ms 83.903 ms 84.032 ms
14 66.171.121.34 <www.fortinet.com> 83.874 ms 84.084 ms 83.810 ms
```

## Checking the logs

A log message records the traffic passing through FortiGate to your network and the action FortiGate takes when it scans the traffic. You should log as much information as possible when you first configure FortiOS. If FortiGate logs are too large, you can turn off or scale back the logging for features that are not in use.

It is difficult to troubleshoot logs without a baseline. Before you can determine if the logs indicate a problem, you need to know what logs result from normal operation.

### When troubleshooting with log files

- Compare current logs to a recorded baseline of normal operation.
- If you need to, increase the level of logging (such as from Warning to Information) to obtain more information.

When increasing logging levels, ensure that you configure email alerts and select both disk usage and log quota. This ensures that you will be notified if the increase in logging causes problems.

#### To configure the log settings in the GUI:

1. Go to *Log & Report > Log Settings*.
2. Determine the activities that generate the most log entries:
  - Check all logs to ensure important information is not overlooked.
  - Filter or order log entries based on different fields, such as level, service, or IP address, to look for patterns that may indicate a specific problem, such as frequent blocked connections on a specific port for all IP addresses.Logs can help identify and locate any problems, but they do not solve them. The purpose of logs is to speed up your problem solving and save you time and effort.  
For more information about logging and log reports, see [Log and Report on page 1618](#).

## Verifying routing table contents in NAT mode

Verify the contents of the routing table when a FortiGate has limited or no connectivity.

The routing table stores the routes currently in use for both static and dynamic protocols. Storing a route in the routing table saves time and resources performing a lookup. To ensure the most recently used routes remain in the table, old routes are bumped to make room for new ones. You cannot perform this task when FortiGate is in transparent mode.

If FortiGate is running in NAT mode, verify that all desired routes are in the routing table, including local subnets, default routes, specific static routes, and dynamic routing protocols.

#### To view the routing table in the GUI:

1. Go to *Monitor > Routing Monitor*.

#### To view the routing table in the CLI:

```
get router info routing-table all
```

#### Sample output:

```
FGT# get router info routing-table all
Codes:
```

```
K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
S* 0.0.0.0/0 [10/0] via 172.20.120.2, wan1
C 10.31.101.0/24 is directly connected, internal
C 172.20.120.0/24 is directly connected, wan1
```

## Verifying the correct route is being used

Run a trace route from a machine in the local area network (LAN) to ensure traffic is flowing as expected through the correct route when there is more than one default route.

In the following example output:

- The first hop contains the IP address 10.10.1.99, which is the internal interface of the FortiGate.
- The second hop contains the IP address 172.20.120.2, to which the wan1 interface of the FortiGate is connected.

This means the route through the wan1 interface is being used for this traffic.

```
C:\>tracert www.fortinet.com
Tracing route to www.fortinet.com [66.171.121.34]
over a maximum of 30 hops:
 1 <1 ms <1 ms <1 ms 10.10.1.99
 2 1 ms <1 ms <1 ms 172.20.120.2
 3 3 ms 3 ms 3 ms static-209-87-254-221.storm.ca [209.87.254.221]
 4 3 ms 3 ms 3 ms core-2-g0-2.storm.ca [209.87.239.129]
 5 13 ms 13 ms 13 ms core-3-bdi1739.storm.ca [209.87.239.199]
 6 12 ms 19 ms 11 ms v502.core1.tor1.he.net [216.66.41.113]
 7 22 ms 22 ms 21 ms 100ge1-2.core1.nyc4.he.net [184.105.80.9]
 8 84 ms 84 ms 84 ms ny-paix-gni.twgate.net [198.32.118.41]
 9 82 ms 84 ms 82 ms 217-228-160-203.TWGATE-IP.twgate.net [203.160.22
8.217]
10 82 ms 81 ms 82 ms 229-228-160-203.TWGATE-IP.twgate.net [203.160.22
8.229]
11 82 ms 82 ms 82 ms 203.78.181.2
12 84 ms 83 ms 83 ms 203.78.186.70
13 84 ms * 85 ms 66.171.127.177
14 84 ms 84 ms 84 ms fortinet.com [66.171.121.34]
15 84 ms 84 ms 83 ms fortinet.com [66.171.121.34]
```

You can also see the route taken for each session by debugging the packet flow in the CLI. For more information, see [Debugging the packet flow on page 1707](#)

## Verifying the correct firewall policy is being used

If you have more than one firewall policy, you can check which policy is being used in the *Policy & Objects* module in the GUI.

**To verify the firewall policy in the GUI:**

1. Go to:
  - *Policy & Objects > IPv4 Policy.*or
  - *Policy & Objects > IPv6 Policy.*
2. Look in the *Count* column to see which policy is being used. The count must show traffic increasing.

Debugging the packet flow in the CLI shows the policy ID that's allowing the traffic. For information, see [Debugging the packet flow on page 1707](#).

## Checking the bridging information in transparent mode

Checking the bridging information is useful when you are experiencing connectivity problems. When FortiGate is set to transparent mode, it acts like a bridge and sends all incoming traffic out on the other interfaces. Each bridge is a link between interfaces.

When traffic is flowing between the interfaces, you can see the bridges listed in the CLI. If no bridges are listed, this is the likely cause of the connectivity issue. When investigating bridging information, check for the MAC address of the interface or device in question.

### How to check the bridging information

**To view the list of bridge instances in the CLI:**

```
diagnose netlink brctl list
```

**Sample output:**

```
#diagnose netlink brctl list
list bridge information
1. root.b fdb: size=256 used=6 num=7 depth=2 simple=no
Total 1 bridges
```

### How to display forwarding domain information

You can use forwarding domains, or collision domains, in routing to limit where packets are forwarded on the network. Layer 2 broadcasts are limited to the same group. By default, all interfaces are in group 0. For example, if the FortiGate has 12 interfaces, only two may be in the same forwarding domain, which limits packets that are broadcast to those two interfaces. This reduces traffic on the rest of the network.

Collision domains prevent the forwarding of ARP packets to all VLANs on an interface. Without collision domains, duplicate MAC addresses on VLANs may cause ARP packets to be duplicated. Duplicate ARP packets can cause some switches to reset. It's important to know what interfaces are part of which forwarding domains because this determines which interfaces can communicate with each other.

**To manually configure forwarding domains in transparent mode in the CLI:**

```
config system interface
 edit <interface_name>
 set forward-domain <integer>
```

end

### To display the forward domains information in the CLI:

```
diagnose netlink brctl domain <name> <id>
```

Where <name> is the name of the forwarding domain to display and <id> is the domain ID.

### Sample output:

```
diagnose netlink brctl domain ione 101
show bridge root.b ione forward domain.
id=101 dev=trunk_1 6
```

### To list the existing bridge MAC table in the CLI:

```
diagnose netlink brctl name host <name>
```

### Sample output:

```
show bridge control interface root.b host.
fdb: size=256, used=6, num=7, depth=2, simple=no
Bridge root.b host table
```

port no	device	devname	mac addr	tth	attributes
2	7	wan2	02:09:0f:78:69:00	0	Local Static
5	6	vlan_1	02:09:0f:78:69:01	0	Local Static
3	8	dmz	02:09:0f:78:69:01	0	Local Static
4	9	internal	02:09:0f:78:69:02	0	Local Static
3	8	dmz	00:80:c8:39:87:5a	194	
4	9	internal	02:09:0f:78:67:68	8	
1	3	wan1	00:09:0f:78:69:fe	0	Local Static

### To list the existing bridge port list in the CLI:

```
diagnose netlink brctl name port <name>
```

### Sample output:

```
show bridge root.b data port.
trunk_1 peer_dev=0
internal peer_dev=0
dmz peer_dev=0
wan2 peer_dev=0
wan1 peer_dev=0
```

## Checking wireless information

Check wireless connections, stations, and interfaces when the problem is not caused by a physical interface.

## Troubleshooting station connection issues

### To check if a station entry is created on access control in the CLI:

```
FG600B3909600253 # diagnose wireless-controller wlac -d sta
* vf=0 wtp=70 rId=2 wlan=open ip=0.0.0.0 mac=00:09:0f:db:c4:03 rssi=0 idle=148 bw=0 use=2
vf=0 wtp=70 rId=2 wlan=open ip=172.30.32.122 mac=00:25:9c:e0:47:88 rssi=-40 idle=0 bw=9
use=2
```

### Enabling diagnostics for a specific station

This example uses the station MAC address to find where it is failing:

```
FG600B3909600253 # diagnose wireless-controller wlac sta_filter 00:25:9c:e0:47:88 1
Set filter sta 00:25:9c:e0:47:88 level 1
FG600B3909600253 # 71419.245 <ih> IEEE 802.11 mgmt::disassoc <== 00:25:9c:e0:47:88 vap open
rId 1 wId 0 00:09:0f:db:c4:03
71419.246 <dc> STA del 00:25:9c:e0:47:88 vap open rId 1 wId 0
71419.246 <cc> STA_CFG_REQ(34) sta 00:25:9c:e0:47:88 del ==> ws (0-192.168.35.1:5246) rId 1
wId 0
71419.246 <cc> STA del 00:25:9c:e0:47:88 vap open ws (0-192.168.35.1:5246) rId 1 wId 0
00:09:0f:db:c4:03 sec open reason I2C_STA_DEL
71419.247 <cc> STA_CFG_RESP(34) 00:25:9c:e0:47:88 <== ws (0-192.168.35.1:5246) rc 0
(Success).
```

## Performing a sniffer trace (CLI and packet capture)

When you troubleshoot networks and routing in particular, it helps to look inside the headers of packets to determine if they are traveling the route that you expect them to take. Packet sniffing is also known as network tap, packet capture, or logic analyzing.



For FortiGates with NP2, NP4, or NP6 interfaces that are offloading traffic, disable offloading on these interfaces before you perform a trace or it will change the sniffer trace.

### Sniffing packets

#### To perform a sniffer trace in the CLI:

Before you start sniffing packets, you should prepare to capture the output to a file. A large amount of data may scroll by and you will not be able to see it without saving it first. One method is to use a terminal program like puTTY to connect to the FortiGate CLI. Once the packet sniffing count is reached, you can end the session and analyze the output in the file.

The general form of the internal FortiOS packet sniffer command is:

```
diagnose sniffer packet <interface_name> <'filter'> <verbose> <count> <tsformat>
```

To stop the sniffer, type CTRL+C.

<b>&lt;interface_name&gt;</b>	The name of the interface to sniff, such as <code>port1</code> or <code>internal</code> . This can also be <code>any</code> to sniff all interfaces.
<b>&lt;'filter'&gt;</b>	What to look for in the information the sniffer reads. <code>none</code> indicates no filtering, and all packets are displayed as the other arguments indicate.  The filter must be inside single quotes (').
<b>&lt;verbose&gt;</b>	The level of verbosity as one of:  <ol style="list-style-type: none"> <li>1 - print header of packets</li> <li>2 - print header and data from IP of packets</li> <li>3 - print header and data from Ethernet of packets</li> <li>4 - print header of packets with interface name</li> </ol>
<b>&lt;count&gt;</b>	The number of packets the sniffer reads before stopping. If you don't put a number here, the sniffer will run until you stop it with <code>&lt;CTRL+C&gt;</code> .
<b>&lt;tsformat&gt;</b>	The timestamp format. <ul style="list-style-type: none"> <li>• <code>a</code>: absolute UTC time, <code>yyyy-mm-dd hh:mm:ss.ms</code></li> <li>• <code>l</code>: absolute LOCAL time, <code>yyyy-mm-dd hh:mm:ss.ms</code></li> <li>• <code>otherwise</code>: relative to the start of sniffing, <code>ss.ms</code></li> </ul>

### Simple sniffing example:

```
diagnose sniffer packet port1 none 1 3.
```

This displays the next three packets on the `port1` interface using no filtering, and verbose level 1. At this verbosity level, you can see the source IP and port, the destination IP and port, action (such as `ack`), and sequence numbers.

In the output below, port 443 indicates these are HTTPS packets and that 172.20.120.17 is both sending and receiving traffic.

```
Head_Office_620b # diagnose sniffer packet port1 none 1 3
interfaces=[port1]
filters=[none]
0.545306 172.20.120.17.52989 -> 172.20.120.141.443: psh 3177924955 ack 1854307757
0.545963 172.20.120.141.443 -> 172.20.120.17.52989: psh 1854307757 ack 3177925808
0.562409 172.20.120.17.52988 -> 172.20.120.141.443: psh 4225311614 ack 3314279933
```

### Advanced sniffing example:

The following commands will report packets on any interface that are traveling between a computer with the host name of "PC1" and a computer with the host name of "PC2". With verbosity 4 and above, the sniffer trace displays the interface names where traffic enters or leaves the FortiGate unit. To stop the sniffer, type `CTRL+C`.

```
FGT# diagnose sniffer packet any "host <PC1> or host <PC2>" 4
or
FGT# diagnose sniffer packet any "(host <PC1> or host <PC2>) and icmp" 4
```

The following CLI command for a sniffer includes the ARP protocol in the filter which may be useful to troubleshoot a failure in the ARP resolution. For example, PC2 may be down and not responding to the FortiGate ARP requests.

```
FGT# diagnose sniffer packet any "host <PC1> or host <PC2> or arp" 4
```

## Using packet capture

To use packet capture, the FortiGate must have a disk. You can enable the `capture-packet` in the firewall policy.

### To enable packet capture in the CLI:

```
config firewall policy
 edit <id>
 set capture-packet enable
end
```

### To configure packet capture filters in the GUI:

Go to *Network > Packet Capture*.

When you add a packet capture filter, enter the following information and click *OK*.

<b>Interface</b>	Select the interface to sniff from the drop-down menu. You must select one interface. You cannot change the interface without deleting the filter and creating a new one, unlike the other fields.
<b>Max Packets to Save</b>	Enter the number of packets to capture before the filter stops. This number cannot be zero. You can halt the capturing before this number is reached.
<b>Enable Filters</b>	Select this option to specify filter fields.
<b>Host(s)</b>	Enter the IP address of one or more hosts. Separate multiple hosts with commas. To enter a range, use a dash without spaces. For example, 172.16.1.5-172.16.1.15, or enter a subnet.
<b>Port(s)</b>	Enter one or more ports to capture on the selected interface. Separate multiple ports with commas. To enter a range, use a dash without spaces, for example 88-90.
<b>VLAN(s)</b>	Enter one or more VLANs (if any). Separate multiple VLANs with commas.
<b>Protocol</b>	Enter one or more protocols. Separate multiple protocols with commas. To enter a range, use a dash without spaces. For example, 1-6, 17, 21-25.
<b>Include IPv6 Packets</b>	Select this option if you are troubleshooting IPv6 networking, or if your network uses IPv6. Otherwise, leave it disabled.
<b>Include Non-IP Packets</b>	The protocols in the list are all IP based except for ICMP (ping). Use this feature to capture non-IP based packets. Examples of non-IP packets include IPsec, IGMP, ARP, and ICMP.

### Managing filters

If you select a filter, you have the option to start and stop packet capture in the edit window, or download the captured packets. You can also see the filter status and the number of packets captured.

You can select the filter and start capturing packets. When the filter is running, the number of captured packets increases until it reaches the *Max Packet Count* or you stop it. You cannot download the output file while the filter is running.



## Packet capture controls

To start, stop, or resume packet capture, use the symbols on the screen. These symbols are the same as those used for audio or video playback. Hover over the symbol to reveal explanatory text. Similarly, to download the \*.pcap file, use the download symbol on the screen.

## Downloading the file

You can download the \*.pcap file when the packet capture is complete. You must use a third party application, such as Wireshark, to read \*.pcap files. This tool provides you with extensive analytics and the full contents of the packets that were captured.

## Debugging the packet flow

Debug the packet flow when network traffic is not entering and leaving the FortiGate as expected. Debugging the packet flow can only be done in the CLI. Each command configures a part of the debug action. The final commands starts the debug.

### To trace the packet flow in the CLI:

```
diagnose debug flow trace start
```

### To follow packet flow by setting a flow filter:

```
diagnose debug flow {filter | filter6} <option>
```

- Enter `filter` if your network uses IPv4.
- Enter `filter6` if your network uses IPv6.

Replace `<option>` with one of the following variables:

Variable	Description
<code>addr</code>	IPv4 or IPv6 address
<code>clear</code>	clear filter
<code>daddr</code>	destination IPv4 or IPv6 address
<code>dport</code>	destination port
<code>negate</code>	inverse IPv4 or IPv6 filter
<code>port</code>	port
<code>proto</code>	protocol number
<code>saddr</code>	source address
<code>sport</code>	source port
<code>vd</code>	index of virtual domain; -1 matches all



If FortiGate is connected to FortiAnalyzer or FortiCloud, the diagnose debug flow output will be recorded as event log messages and then sent to the devices. Do not run this command longer than necessary, as it generates a significant amount of data.



FortiASIC NP4 or NP6 interface pairs that offload traffic will change the packet flow. Before debugging any NP4 or NP6 interfaces, disable offloading on those interfaces.

To do this, enter `diagnose npu <interface pair> fastpath disable`, where `interface pair` is `np4,np6,np4lite`, or `np6lite`.

### To start flow monitoring with a specific number of packets:

```
diagnose debug flow trace start <N>
```

### To stop flow tracing at any time:

```
diagnose debug flow trace stop
```

The following example shows the flow trace for a device with an IP address of 203.160.224.97:

```
diagnose debug enable
diagnose debug flow filter addr 203.160.224.97
diagnose debug flow show function-name enable
diagnose debug flow trace start 100
```

### Sample output: HTTP

To observe the debug flow trace, connect to the website at the following address:

```
https://www.fortinet.com
```

Comment: SYN packet received:

```
id=20085 trace_id=209 func=resolve_ip_tuple_fast
line=2700 msg="vd-root received a packet(proto=6,
192.168.3.221:1487->203.160.224.97:80) from port5."
```

SYN sent and a new session is allocated:

```
id=20085 trace_id=209 func=resolve_ip_tuple line=2799
msg="allocate a new session-00000e90"
```

Lookup for next-hop gateway address:

```
id=20085 trace_id=209 func=vf_ip4_route_input line=1543
msg="find a route: gw-192.168.11.254 via port6"
```

Source NAT, lookup next available port:

```
id=20085 trace_id=209 func=get_new_addr line=1219
msg="find SNAT: IP-192.168.11.59, port-31925"
direction"
```

Matched security policy. Check to see which policy this session matches:

```
id=20085 trace_id=209 func=fw_forward_handler line=317
msg="Allowed by Policy-3: SNAT"
```

**Apply source NAT:**

```
id=20085 trace_id=209 func=__ip_session_run_tuple
line=1502 msg="SNAT 192.168.3.221->192.168.11.59:31925"
```

**SYN ACK received:**

```
id=20085 trace_id=210 func=resolve_ip_tuple_fast line=2700
msg="vd-root received a packet(proto=6, 203.160.224.97:80-
>192.168.11.59:31925) from port6."
```

**Found existing session ID. Identified as the reply direction:**

```
id=20085 trace_id=210 func=resolve_ip_tuple_fast line=2727
msg="Find an existing session, id-00000e90, reply direction"
```

**Apply destination NAT to inverse source NAT action:**

```
id=20085 trace_id=210 func=__ip_session_run_tuple
line=1516 msg="DNAT 192.168.11.59:31925-
>192.168.3.221:1487"
```

**Lookup for next-hop gateway address for reply traffic:**

```
id=20085 trace_id=210 func=vf_ip4_route_input line=1543
msg="find a route: gw-192.168.3.221 via port5"
```

**ACK received:**

```
id=20085 trace_id=211 func=resolve_ip_tuple_fast line=2700
msg="vd-root received a packet(proto=6,
192.168.3.221:1487->203.160.224.97:80) from port5."
```

**Match existing session in the original direction:**

```
id=20085 trace_id=211 func=resolve_ip_tuple_fast line=2727
msg="Find an existing session, id-00000e90, original
direction"
```

**Apply source NAT:**

```
id=20085 trace_id=211 func=__ip_session_run_tuple
line=1502 msg="SNAT 192.168.3.221->192.168.11.59:31925"
```

**Receive data from client:**

```
id=20085 trace_id=212 func=resolve_ip_tuple_fast
line=2700 msg="vd-root received a packet(proto=6,
192.168.3.221:1487->203.160.224.97:80) from port5."
```

**Match existing session in the original direction:**

```
id=20085 trace_id=212 func=resolve_ip_tuple_fast
line=2727 msg="Find an existing session, id-00000e90,
original direction"
```

**Apply source NAT:**

```
id=20085 trace_id=212 func=__ip_session_run_tuple
line=1502 msg="SNAT 192.168.3.221->192.168.11.59:31925"
```

**Receive data from server:**

```
id=20085 trace_id=213 func=resolve_ip_tuple_fast
line=2700 msg="vd-root received a packet(proto=6,
203.160.224.97:80->192.168.11.59:31925) from port6."
```

Match existing session in reply direction:

```
id=20085 trace_id=213 func=resolve_ip_tuple_fast
line=2727 msg="Find an existing session, id-00000e90,
reply direction"
```

Apply destination NAT to inverse source NAT action:

```
id=20085 trace_id=213 func=__ip_session_run_tuple
line=1516 msg="DNAT 192.168.11.59:31925-
>192.168.3.221:1487"
```

### Sample output: IPsec (policy-based)

```
id=20085 trace_id=1 msg="vd-root received a packet(proto=1, 10.72.55.240:1->10.71.55.10:8)
from internal."
id=20085 trace_id=1 msg="allocate a new session-00001cd3"
id=20085 trace_id=1 msg="find a route: gw-66.236.56.230 via wan1"
id=20085 trace_id=1 msg="Allowed by Policy-2: encrypt"
id=20085 trace_id=1 msg="enter IPsec tunnel-RemotePhase1"
id=20085 trace_id=1 msg="encrypted, and send to 15.215.225.22 with source 66.236.56.226"
id=20085 trace_id=1 msg="send to 66.236.56.230 via intf-wan1"
id=20085 trace_id=2 msg="vd-root received a packet (proto=1, 10.72.55.240:1-1071.55.10:8)
from internal."
id=20085 trace_id=2 msg="Find an existing session, id-00001cd3, original direction"
id=20085 trace_id=2 msg="enter IPsec ="encrypted, and send to 15.215.225.22 with source
66.236.56.226" tunnel-RemotePhase1"
id=20085 trace_id=2 msgid=20085 trace_id=2 msg="send to 66.236.56.230 via intf-wan1"
```

## Testing a proxy operation

**To monitor proxy operations in the CLI:**

```
diagnose test application <application> <option>
```

**To display a list of available application values:**

```
diagnose test application ?
```

**To display a list of available option values:**

```
diagnose test application <application> ?
```

The <option> value will depend on the application value used in the command.

For example, if the application is http, the CLI command that displays the <option> values is:

```
diagnose test application http ?
```

## Displaying detail Hardware NIC information

Monitoring the hardware NIC is important because interface errors indicate data link or physical layer issues which may impact the performance of the FortiGate.

## To monitor hardware network operations in the CLI:

```
diagnose hardware deviceinfo nic <interface>
```

### Sample output:

The following is sample output when the <interface> is set to lan:

```
System_Device_Name lan
Current_HWaddr 00:09:0f:68:35:60
Permanent_HWaddr 00:09:0f:68:35:60
State up
Link up
Speed 100
Duplex full
[.....]
Rx_Packets=5685708
Tx_Packets=4107073
Rx_Bytes=617908014
Tx_Bytes=1269751248
Rx_Errors=0
Tx_Errors=0
Rx_Dropped=0
Tx_Dropped=0
[.....]
```

### Error descriptions

The `diagnose hardware deviceinfo nic` command displays a list of error names and values that are related to hardware.

The following table describes possible hardware errors:

Field	Description
Rx_Errors = rx error count	Bad frame was marked as error by PHY
Rx_CRC_Errors + Rx_Length_Errors - Rx_Align_Errors	This error is only valid in 10/100M mode
Rx_Dropped or Rx_No_Buffer_Count	Running out of buffer space
Rx_Missed_Errors	Equals Rx_FIFO_Errors + CEXTERR (Carrier Extension Error Count); only valid in 1000M mode, which is marked by PHY
Tx_Errors = Tx_Aborted_Errors	ECOL (Excessive Collisions Count); only valid in half-duplex mode
Tx_Window_Errors	Late Collisions (LATECOL) Count

Field	Description
	Late collisions are collisions that occur after 64-byte time into the transmission of the packet while working in 10 to 100 Mb/s data rate and 512-byte time into the transmission of the packet while working in the 1,000 Mb/s data rate. This register only increments if transmits are enabled and the device is in half-duplex mode.
Rx_Dropped	See Rx_Errors
Tx_Dropped	Not defined
Collisions	Total number of collisions experienced by the transmitter; valid in half-duplex mode
Rx_Length_Errors	Transmission length error
Rx_Over_Errors	Not defined
Rx_CRC_Errors	Frame CRC error
Rx_Frame_Errors	Same as Rx_Align_Errors This error is only valid in 10/100M mode.
Rx_FIFO_Errors	Same as Rx_Missed_Errors - a missed packet count
Tx_Aborted_Errors	See Tx_Errors
Tx_Carrier_Errors	The PHY should assert the internal carrier sense signal during every transmission. Failure to do so may indicate that the link has failed or the PHY has an incorrect link configuration. This register only increments if transmits are enabled. This register isn't valid in internal SerDes 1 mode (TBI mode for the 82544GC/EI) and is valid only when the Ethernet controller is operating at full duplex.
Tx_FIFO_Errors	Not defined
Tx_Heartbeat_Errors	Not defined
Tx_Window_Errors	See LATECOL
Tx_Single_Collision_Frames	Counts the number of times that a successfully transmitted packet encountered a single collision The value increments only if transmits are enabled and the Ethernet controller is in half-duplex mode.
Tx_Multiple_Collision_Frames	A Multiple Collision Count which indicates the number of times that a transmit encountered more than one collision, but less than 16. The value increments only if transmits are enabled and the Ethernet controller is in half-duplex mode.
Tx_Deferred	Counts defer events. A deferred event occurs when the transmitter cannot immediately send a packet due to: <ul style="list-style-type: none"> <li>• The medium being busy because another device is transmitting</li> <li>• The IPG timer hasn't expired</li> <li>• Half-duplex deferral events are occurring</li> <li>• XOFF frames are being received</li> <li>• he link is not up.</li> </ul>

Field	Description
	This register only increments if transmits are enabled. This counter does not increment for streaming transmits that are deferred due to TX IPG.
Rx_Frame_Too_Longs	The Rx frame is oversized
Rx_Frame_Too_Shots	The Rx frame is too short
Rx_Align_Errors	This error is only valid in 10/100M mode
Symbol Error Count	Counts the number of symbol errors between reads - SYMERRS. The count increases for every bad symbol that's received, whether or not a packet is currently being received and whether or not the link is up. This register increments only in internal SerDes mode.

## Performing a traffic trace

Traffic tracing allows you to follow a specific packet stream. This is useful when you want to confirm that packets are using the route you expect them to take on your network.

### To view traffic sessions:

Use this command to view the characteristics of a traffic session through specific security policies.

```
diagnose sys session
```

### To trace per-packet operations for flow tracing:

```
diagnose debug flow
```

### To trace per-Ethernet frame:

```
diagnose sniffer packet
```

### To trace a route from a FortiGate to a destination IP address:

```
execute traceroute www.fortinet.com
traceroute to www.fortinet.com (66.171.121.34), 32 hops max, 84 byte packets
1 172.20.120.2 0.637 ms 0.653 ms 0.279 ms
2 209.87.254.221 <static-209-87-254-221.storm.ca> 2.448 ms 2.519 ms 2.458 ms
3 209.87.239.129 <core-2-g0-2.storm.ca> 2.917 ms 2.828 ms 9.324 ms
4 209.87.239.199 <core-3-bdi1739.storm.ca> 13.248 ms 12.401 ms 13.009 ms
5 216.66.41.113 <v502.core1.tor1.he.net> 17.181 ms 12.422 ms 12.268 ms
6 184.105.80.9 <100ge1-2.core1.nyc4.he.net> 21.355 ms 21.518 ms 21.597 ms
7 198.32.118.41 <ny-paix-gni.twgate.net> 83.297 ms 84.416 ms 83.782 ms
8 203.160.228.217 <217-228-160-203.TWGATE-IP.twgate.net> 82.579 ms 82.187 ms 82.066 ms
9 203.160.228.229 <229-228-160-203.TWGATE-IP.twgate.net> 82.055 ms 82.455 ms 81.808 ms
10 203.78.181.2 82.262 ms 81.572 ms 82.015 ms
11 203.78.186.70 83.283 ms 83.243 ms 83.293 ms
12 66.171.127.177 84.030 ms 84.229 ms 83.550 ms
13 66.171.121.34 <www.fortinet.com> 84.023 ms 83.903 ms 84.032 ms
```

14 66.171.121.34 <www.fortinet.com> 83.874 ms 84.084 ms 83.810 ms

## Using a session table

A session is a communication channel between two devices or applications across the network. Sessions allow FortiOS to inspect and act on a sequential group of packets in a session all at once instead of inspecting each packet individually. Each session has an entry in the session table that includes important information about the session.

You can view FortiGate session tables from the FortiGate GUI or CLI. The most useful troubleshooting data comes from the CLI. The session table in the GUI also provides useful summary information, particularly the current policy number that the session is using.

### When to use a session table

Session tables are useful when verifying open connections. For example, if you have a web browser open to browse the Fortinet website, you would expect a session entry from your computer on port 80 to the IP address for the Fortinet website.

You can also use a session table to investigate why there are too many sessions for FortiOS to process.

### GUI

To view session information, go to the *FortiView* page.

For information about FortiView consoles, see [FortiView on page 276](#).

### Finding the security policy for a specific connection

Every program and device on your network must have an open communication channel or session to pass information. FortiGate manages these sessions with features such as traffic shaping, antivirus scanning, and blocking known bad websites. Each session will have an entry in the session table.

If a secure web browser session is not working properly, you can check the session table to ensure the session is still active and going to the proper address. The session table can also tell you the security policy number it matches, so you can check what is happening in that policy.

#### 1. Get the connection information.

You need to be able to identify the session you want. To do this, you will need:

- The source IP address (usually your computer)
- The destination IP address (if you have it)
- The port number which is determined by the program you are using. Common ports are:
  - Port 80 (HTTP for web browsing)
  - Port 443 (HTTPS for SSL encrypted web browsing)
  - Port 22 (SSH for Secure Shell)
  - Port 25 (SMTP for Mail Transfer)

#### 2. Find the session and policy ID

Go to *FortiView > All Sessions*.



To find your session, search for your source IP address, destination IP address (if you have it), and port number. The policy ID is listed after the destination information.

### 3. Use filters to find a session

If there are multiple pages of sessions, you can use a filter to hide the sessions you do not need. To filter the sessions in the table, click *Add Filter*, and select an option from the list. You can filter the table by *Destination IP*, *Source IP*, or *Source Port*.

## CLI

The session table output in the CLI is very large. The CLI command supports filters to show only the data you need.

### To view session data in the CLI:

```
diagnose sys session list
```

An entry is placed in the session table for each traffic session passing through a security policy

### To filter session data:

```
diagnose sys session filter <option>
```

The values for <option> include the following:

Value	Definition
clear	Clear session filter
dintf	Destination interface
dport	Destination port
dst	Destination IP address
duration	Duration of the session
expire	Expire
negate	Inverse filter
nport	NAT'd source port
nsrc	NAT'd source ip address
policy	Policy ID
proto	Protocol number
proto-state	Protocol state
session-state1	Session state1
session-state2	Session state2
sintf	Source interface
sport	Source port

Value	Definition
src	Source IP address
vd	Index of virtual domain, -1 matches all

Even though UDP is a sessionless protocol, FortiGate keeps track of the following states:

- When UDP reply does not have a value of 0
- When UDP reply has a value of 1

The following table displays firewall session states from the session table:

State	Description
log	Session is being logged
local	Session is originated from or destined for local stack
ext	Session is created by a firewall session helper
may_dirty	Session is created by a policy For example, the session for <code>ftp control channel</code> will have this state but <code>ftp data channel</code> won't. This is also seen when NAT is enabled.
ndr	Session will be checked by IPS signature
nds	Session will be checked by IPS anomaly
br	Session is being bridged (TP) mode

## Examining the firewall session list

The firewall session list displays all open sessions in FortiGate. Examine the list for strange patterns, such as no sessions apart from the internal network, or all sessions are only to one IP address.

When you examine the firewall session list in the CLI, you can use filters to reduce the output. In the GUI, the filters are part of the interface.

### To examine the firewall session list in the GUI:

Go to *FortiView > All Sessions*.

### To examine the firewall session list in the CLI:

You can use a filter to limit the sessions displayed by source, destination address, port, or NAT'd address. To use more than one filter, enter a separate line for each value.

The following example filters the session list based on a source address of 10.11.101.112:

```
FGT# diagnose sys session filter src 10.11.101.112
FGT# diagnose sys session list
```

The following example filters the session list based on a destination address of 172.20.120.222.

```
FGT# diagnose sys session filter dst 172.20.120.222
FGT# diagnose sys session list
```

To clear all sessions corresponding to a filter:

```
FGT# diagnose sys session filter dst 172.20.120.222
FGT# diagnose sys session clear
```

## Checking source NAT information

Checking source NAT is important when you are troubleshooting from the remote end of the connection outside the firewall.

### To check the source NAT information in the GUI:

1. Go to *FortiView > All Sessions*.
2. Check the values in the *Source Nat Address* and *Source Nat Port* columns. These columns display the IP and port values after NAT has been applied.

Checking the NAT values can help you confirm they are the values you expect, and to ensure the remote end of the sessions can see the expected IP address and port number.

### To check the source NAT information in the CLI:

When you display the session list in the CLI, you can match the NAT'd source address (`nsrc`) and port (`nport`). This is useful when multiple internal IP addresses are NAT'd to a common external-facing source IP address.

```
FGT# diagnose sys session filter nsrc 172.20.120.122
FGT# diagnose sys session filter nport 8888
FGT# diagnose sys session list
```

## Finding object dependencies

You may be prevented from deleting a configuration object when other configuration objects depend on it. You can use the GUI or CLI to identify objects which depend on, or make reference to the configuration you are trying to delete. Additionally, if you have a virtual interface with dependent objects, you will need to find and remove those dependencies before deleting the interface.

### To remove interface object dependencies in the GUI:

1. Go to *Network > Interfaces*. The *Ref.* column displays the number of objects that reference this interface.
2. Select the number in the *Ref.* column for the interface. A window listing the dependencies appears.
3. Use these detailed entries to locate and remove object references to this interface. The trash can icon is enabled after all the object dependencies are removed.
4. Remove the interface by selecting the check box for the interface, and select *Delete*.

### To find object dependencies in the CLI:

When running multiple VDOMs, use the following command in the global configuration only.

```
diagnose sys cmd db refcnt show <path.object.mkey>
```

The command searches for the named object in both the most recently used global and VDOM configurations.

## Examples

To verify which objects a security policy with an ID of 1 refers to:

```
diagnose sys cmdb refcnt show firewall.policy.policyid 1
```

To check what is referred to by interface port1:

```
diagnose sys cmdb refcnt show system.interface.name port1
```

To show all dependencies for an interface:

```
diagnose sys cmdb refcnt show system.interface.name <interface name>
```

## Sample output:

In this example, the interface has dependent objects, including four address objects, one VIP, and three security policies.

```
entry used by table firewall.address:name '10.98.23.23_host'
entry used by table firewall.address:name 'NAS'
entry used by table firewall.address:name 'all'
entry used by table firewall.address:name 'fortinet.com'
entry used by table firewall.vip:name 'TORRENT_10.0.0.70:6883'
entry used by table firewall.policy:policyid '21'
entry used by table firewall.policy:policyid '14'
entry used by table firewall.policy:policyid '19'
```

## Diagnosing NPU-based interfaces

Some Fortinet products contain network processors, such as NP1, NP2, NP4, and NP6. Offloading requirements will vary depending on the model.

### To view the initial session setup for NPU-based interfaces:

```
diagnose debug flow
```

- If the session is programmed into the ASIC (fastpath) correctly, the command will not detect the packets that arrive at the CPU.
- If the NPU functionality is disabled, the CPU detects all the packets. However, you should only disable the NPU functionality for troubleshooting purposes.

### To diagnose NPU-based interfaces:

1. Get the NP4 or NPU ID and port numbers.

```
diagnose npu {np4|npu6}list
```

The output will look like this:

```
ID Model Slot Interface
0 On-board port1 fabric1 fabric3 fabric5
1 On-board fabric2 port2 base2 fabric4
```

2. Disable the NPU functionality.

```
diagnose npu {np4|npu6}fastpath disable <dev_id>
```

The dev\_id is the NP4 or NP6 number.

3. Analyze the packets.

```
diagnose npu {np4|npu6}fastpath-sniffer enable port1
```



These commands only apply to the newer NP4 and NP6 interfaces.

The output will look like this:

```
NP4 Fast Path Sniffer on port1 enabled
```

This causes traffic on `port1` of the network processor to be sent to the CPU. This means you can perform a standard sniffer trace and use other diagnostic commands, if it is a standard CPU-driven port.

## Running the TAC report

The Technical Assistance Center (TAC) report runs an exhaustive series of diagnostic commands. Some of the commands are only needed if you are using features, such as HA, VPN tunnels, or a modem. Fortinet support may ask you to use the report output to provide information about the current state of your FortiGate.

Due to the amount of output generated, the report may take a few minutes to run. If you are logging CLI output to a file, you can run this command to familiarize yourself with the diagnostic commands.

**To run the TAC report in the CLI:**

```
exec tac report
```

## Other commands

You may be asked to provide the following information when you contact Fortinet support.

- [ARP table on page 1719](#)
- [IP address on page 1721](#)

### ARP table

The ARP table is used to determine the destination MAC addresses of the network nodes, as well as the VLANs and ports from where the nodes are reached.

**To view the ARP table:**

```
get system arp
```

Address	Age (min)	Hardware Addr	Interface
10.10.1.3	1	50:b7:c3:75:ea:dd	internal7
192.168.0.190	0	28:f1:0e:03:2a:97	wan1
192.168.0.97	0	f4:f2:6d:37:b0:99	wan1

**To view the ARP cache in the system:**

```
diagnose ip arp list
```

```
index=14 ifname=internal7 10.10.1.3 50:b7:c3:75:ea:dd state=00000004 use=2494 confirm=1995
```

```
update=374 ref=3
index=5 ifname=wan1 192.168.0.190 28:f1:0e:03:2a:97 state=00000002 use=88 confirm=86
update=977639 ref=2
index=22 ifname=internal 192.168.1.111 00:0c:29:c6:79:3d state=00000004 use=3724
confirm=9724 update=3724 ref=0
index=5 ifname=wan1 224.0.1.140 01:00:5e:00:01:8c state=00000040 use=924202 confirm=930202
update=924202 ref=1
index=5 ifname=wan1 192.168.0.97 f4:f2:6d:37:b0:99 state=00000002 use=78 confirm=486
update=614 ref=26
index=14 ifname=internal7 10.10.1.11 state=00000020 use=172 confirm=1037790 update=78 ref=2
```

## ARP request and cache

The FortiGate must make an ARP request when it tries to reach a new destination. The base ARP reachable value determines how often an ARP request it sent; the default is 30 seconds. The actual ARP reachable time is a random number between half and three halves of the base reachable time, or 15 to 45 seconds. The random number is updated every five minutes.

ARP entries in the ARP cache are updated based on the state of the ARP entry and the objects that are using it, as highlighted in the following output sample:

```
index=5 ifname=wan1 224.0.1.140 01:00:5e:00:01:8c state=00000040 use=924202
confirm=930202 update=924202 ref=1
```

There are multiple possible states for an ARP entry, and the state-transition mechanism can be complex. Common states include the following:

State	Meaning	Description
000000002 or 0x02	REACHABLE	An ARP response was received
000000004 or 0x04	STALE	No ARP response within the expected time
000000008 or 0x08	DELAY	A transition state between STALE and REACHABLE before Probes are sent out
000000020 or 0x20	FAILED	Did not manage to resolve within the maximum configured number of probes
000000040 or 0x40	NOARP	Device does not support ARP, e.g. IPsec interface
000000080 or 0x80	PERMANENT	A statically defined ARP entry

An entry that is in the STALE (0x04) or FAILED (0x20) states with no references to it (ref=0) can be deleted. Many factors affect the state-transmit mechanism and if an entry is used by other subsystems. For example, ARP creation, ARP request/reply, neighbor lookup, routing, and others can cause an ARP entry to be in use or referenced.

The garbage collection mechanism runs every 30 seconds, and checks and removes stale and unreferenced entries if they have been stale for longer than 60 seconds. Garbage collection will also be triggered when the number of ARP entries exceeds the configured threshold. If the threshold is exceeded, no entries can be added to the ARP table.

### To set the maximum number of ARP entries threshold:

```
config system global
 set arp-max-entry <integer>
end
```

<code>arp-max-entry &lt;integer&gt;</code>	The maximum number of dynamically learned MAC addresses that can be added to the ARP table (131072 to 2147483647, default = 131072).
--------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------

#### To clear all of the entries in the ARP table:

```
execute clear system arp table
```

#### To delete a single ARP entry from the ARP table:

```
diagnose ip arp delete <interface name> <IP address>
```

#### To add static ARP entries:

```
config system arp-table
 edit 1
 set interface "internal"
 set ip 192.168.50.8
 set mac bc:14:01:e9:77:02
 next
end
```

#### To view a summary of the ARP table:

```
diagnose sys device list root

list virtual firewall root info:
ip4 route_cache: table_size=65536 max_depth=2 used=31 total=34
arp: table_size=16 max_depth=2 used=5 total=6
proxy_arp: table_size=256 max_depth=0 used=0 total=0
arp6: table_size=32 max_depth=1 used=3 total=3
proxy_arp6: table_size=256 max_depth=0 used=0 total=0
local table version=00000000 main table version=0000002b
vf=root dev=root vrf=0
vf=root dev=ssl.root vrf=0
...
vf=root dev=internal5 vrf=0
ses=0/0 ses6=0/0 rt=0/0 rt6=0/0
```

## IP address

You may want to verify the IP addresses assigned to the FortiGate interfaces are what you expect them to be.

#### To verify IP addresses:

```
diagnose ip address list
```

The output lists the:

- IP address and mask (if available)
- index of the interface (a type of ID number)
- devname (the interface name)

While physical interface names are set, virtual interface names can vary. A good way to use this command is to list all of the virtual interface names. For `vsys_ha` and `vsys_fgfm`, the IP addresses are the local host, which are virtual interfaces that are used internally.

#### Sample output:

```
diagnose ip address list
IP=10.31.101.100->10.31.101.100/255.255.255.0 index=3 devname=internal
IP=172.20.120.122->172.20.120.122/255.255.255.0 index=5 devname=wan1
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=8 devname=root
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=11 devname=vsys_ha
IP=127.0.0.1->127.0.0.1/255.0.0.0 index=13 devname=vsys_fgfm
```

## FortiGuard troubleshooting

The FortiGuard service provides updates to AntiVirus (AV), Antispam (AS), Intrusion Protection Services (IPS), Webfiltering (WF), and more. The FortiGuard Distribution System (FDS) consists of a number of servers across the world that provide updates to your FortiGate unit. Problems can occur with the connection to FDS and its configuration on your local FortiGate unit.

Some of the more common troubleshooting methods are listed here, including:

- [Troubleshooting process for FortiGuard updates on page 1723](#)
- [FortiGuard server settings on page 1724](#)
- [FortiGuard server settings on page 1724](#)

### Verifying connectivity to FortiGuard

You can verify FortiGuard connectivity in the GUI and CLI.

#### To verify FortiGuard connectivity in the GUI:

1. Got to *Dashboard > Status*.
2. Check the *Licenses* widget. When FortiGate is connected to FortiGuard, a green check mark appears next to the available FortiGuard services.

#### To verify FortiGuard connectivity in the CLI:

```
execute ping service.fortiguard.net
execute ping update.fortiguard.net
```

#### Sample output:

```
FG100D# execute ping service.fortiguard.net
PING guard.fortinet.net (208.91.112.196): 56 data bytes
64 bytes from 208.91.112.196: icmp_seq=0 ttl=51 time=61.0 ms
64 bytes from 208.91.112.196: icmp_seq=1 ttl=51 time=60.0 ms
64 bytes from 208.91.112.196: icmp_seq=2 ttl=51 time=59.6 ms
64 bytes from 208.91.112.196: icmp_seq=3 ttl=51 time=58.9 ms
64 bytes from 208.91.112.196: icmp_seq=4 ttl=51 time=59.2 ms
```



```
--- guard.fortinet.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 58.9/59.7/61.0 ms
```

```
FG100D# execute ping update.fortiguard.net
PING fdl.fortinet.com (208.91.112.68): 56 data bytes
64 bytes from 208.91.112.68: icmp_seq=0 ttl=53 time=62.0 ms
64 bytes from 208.91.112.68: icmp_seq=1 ttl=53 time=61.8 ms
64 bytes from 208.91.112.68: icmp_seq=2 ttl=53 time=61.3 ms
64 bytes from 208.91.112.68: icmp_seq=3 ttl=53 time=61.9 ms
64 bytes from 208.91.112.68: icmp_seq=4 ttl=53 time=61.8 ms
```

## Troubleshooting process for FortiGuard updates

The following process shows the logical steps you should take when troubleshooting problems with FortiGuard updates:

- 1. Does the device have a valid license that includes these services?**  
Each device requires a valid FortiGuard license to access updates for some or all of these services. You can verify the status of the support contract for your devices at the [Fortinet Support](#) website.
- 2. If the device is part of a high availability (HA) cluster, do all members of the cluster have the same level of support?**  
You can verify the status of the support contract for all of the devices in your HA cluster at the [Fortinet Support](#) website.
- 3. Are services enabled on the device?**  
To see the FortiGuard information and status for a device in the GUI, go to *System > FortiGuard*.  
Use this page to verify the status of each component, and enable each service.
- 4. Can the device communicate with FortiGuard servers?**  
Go to *System > FortiGuard* in the GUI, and try to update AntiVirus and IPS, or test the availability of Web Filtering and AS default and alternate ports.
- 5. Is there proper routing to reach the FortiGuard servers?**  
Ensure there is a static or dynamic route that allows your FortiGate to reach the FortiGuard servers. Usually a generic default route to the internet is enough, but you may need to verify this if your network is complex.
- 6. Are there issues with DNS?**  
An easy way to test this is to attempt a traceroute from behind the FortiGate to an external network using the Fully Qualified Domain Name (FQDN) for a location. If the traceroute FQDN name doesn't resolve, you have general DNS problems.
- 7. Is there anything upstream that might be blocking FortiGuard traffic, either on the network or ISP side?**  
Many firewalls block all ports, by default, and ISPs often block ports that are low. There may be a firewall between the FortiGate and the FortiGuard servers that's blocking the traffic. By default, FortiGuard uses port 53. If that port is blocked you need to either open a hole for it or change the port it is using.
- 8. Is there an issue with source ports?**  
It is possible that ports that FortiGate uses to contact FortiGuard are being changed before they reach FortiGuard or on the return trip before they reach FortiGate. A possible solution for this is to use a fixed-port at NAT'd firewalls to ensure the port remains the same. You can use packet sniffing to find more information about what's happening with ports.
- 9. Are there security policies that include antivirus?**  
If none of the security policies include antivirus, the antivirus database will not be updated. If antivirus is included, only the database type that's used will be updated.

## FortiGuard server settings

Your local FortiGate connects to remote FortiGuard servers to get updates to FortiGuard information, such as new viruses that may have been found or other new threats.

This section provides methods to display FortiGuard server information on your FortiGate, and how to use that information and update it to fix potential problems.

### Displaying the server list

**To get a list of FDS servers FortiGate uses to send web filtering requests:**

```
get webfilter status
```

or

```
diagnose debug rating
```

Rating requests are only sent to the server at the top of the list in normal operation. Each server is probed for Round Trip Time (RTT) every two minutes.

Optionally, you can add a refresh rate to the end of the command to determine how often the server list is refreshed.

Rating may not be enabled on your FortiGate.

#### Sample output:

```
Locale : english
License : Contract
Expiration : Thu Oct 9 02:00:00 2011
== Server List (Mon Feb 18 12:55:48 2008) ==
```

IP	Weight	RTT	Flags	TZ	Packets	CurrLost	TotalLost
a.b.c.d	0	1	DI	2	1926879	0	11176
10.1.101.1	10	329		1	10263	0	633
10.2.102.2	20	169		0	16105	0	80
10.3.103.3	20	182		0	6741	0	776
10.4.104.4	20	184		0	5249	0	987
10.5.105.5	25	181		0	12072	0	178

#### Output details

The server list includes the IP addresses of alternate servers if the first entry cannot be reached. In this example, the IP addresses are not public addresses.

The following flags in `get webfilter status` indicate the server status:

Flag	Description
D	The server was found through the DNS lookup of the hostname.

Flag	Description
	If the hostname returns more than one IP address, all of them are flagged with D and are used first for INIT requests before falling back to the other servers.
I	The server to which the last INIT request was sent
F	The server hasn't responded to requests and is considered to have failed
T	The server is currently being timed
S	<p>Rating requests can be sent to the server.</p> <p>The flag is set for a server only in two cases:</p> <ul style="list-style-type: none"> <li>• The server exists in the servers list received from the (Undefined variable: FortinetVariables.ProductName1) or any other INIT server.</li> <li>• The server list received from the (Undefined variable: FortinetVariables.ProductName1) is empty so the (Undefined variable: FortinetVariables.ProductName1) is the only server that the (Undefined variable: FortinetVariables.ProductName6) knows and it should be used as the rating server.</li> </ul>

### Sorting the server list

The server list is sorted first by weight. The server with the smallest RTT appears at the top of the list, regardless of weight. When a packet is lost (there has been no response in 2 seconds), it is re-sent to the next server in the list. Therefore, the top position in the list is selected based on RTT, while the other positions are based on weight.

### Calculating weight

The weight for each server increases with failed packets and decreases with successful packets. To lower the possibility of using a remote server, the weight isn't allowed to dip below a base weight. The base weight is calculated as the difference in hours between the FortiGate and the server multiplied by 10. The farther away the server is, the higher its base weight is and the lower it appears in the list.

## Additional resources

To learn more about FortiGate and FortiOS, as well information about technical issues, please refer to the following resources:

### Technical documentation

Installation, Administration, and Quick Start Guides, as well as other technical documents, are available online at the [Fortinet Document Library](#)

### Fortinet video library

The [Fortinet Video Library](#) hosts a collection of video which provide valuable information about Fortinet products.

## Release notes

Issues that arise after the technical documentation has been published will often be listed in the Release Notes. To find these, go to the [Fortinet Document Library](#).

## Knowledge base

The [Fortinet Knowledge Base](#) provides access to a variety of articles, white papers, and other documentation that provides technical insight into a range of Fortinet products. The Knowledge Base is available online at: <https://kb.fortinet.com>

## Fortinet technical discussion forums

An [online technical forum](#) allows administrators to contribute to discussions about issues that relate to their Fortinet products. Searching the forum can help an administrator identify if an issue has been experienced by another user. You can access the support forums at: <https://forum.fortinet.com/>

## Fortinet training services online campus

The [Fortinet Training Services Online Campus](#) hosts a collection of tutorials and training materials which you can use to increase your knowledge of Fortinet products. <https://www.fortinet.com/training.html>

## Fortinet Support

You defined your problem, researched a solution, put together a plan to find the solution, and executed that plan. At this point, if the problem hasn't been solved, it's time to contact [Fortinet Support](#) for assistance.



**FORTINET®**



Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.